Cisco Networkers 2009
January 26-29 Barcelona, Spain

Fiber to the Home Access Architectures

BRKBBA-2006

Thomas Martin

© 2009 Cisco Systems, Inc. All rights reserved.
Cisco Public

Housekeeping

- We value your feedback- don't forget to complete your online session evaluations after each session & complete the Overall Conference Evaluation which will be available online from Thursday
- Visit the World of Solutions
- Please remember this is a 'non-smoking' venue!
- Please switch off your mobile phones
- Please make use of the recycling bins provided
- Please remember to wear your badge at all times including the Party

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

AGENDA

Introduction to Fiber to the Home

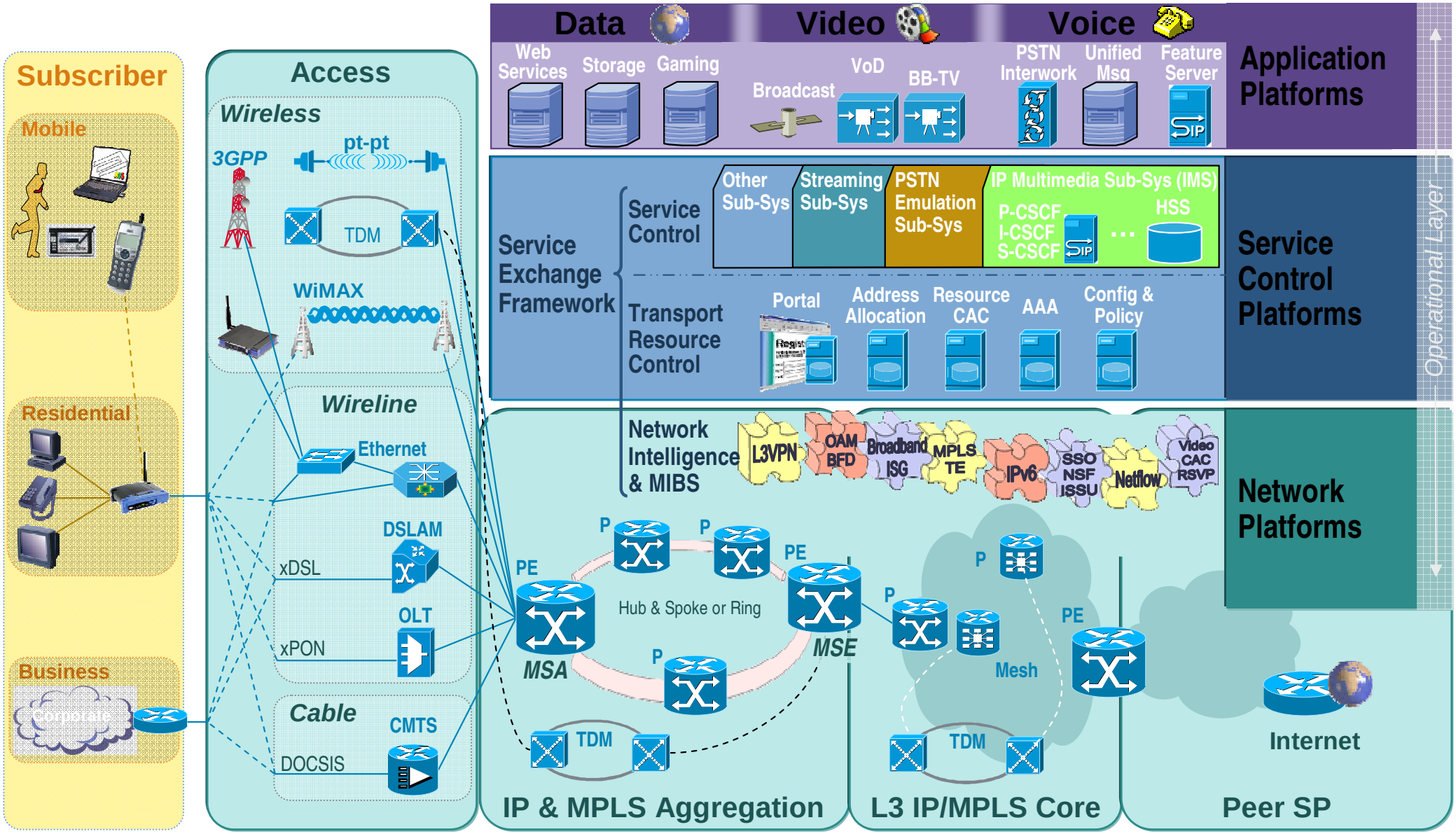
FTTH Technologies

FTTH Deployment Options and Best Practices

FTTH Network Architecture and Design

© 2009 Cisco Systems, Inc. All rights reserved.

SP Next Generation Network Blue Print



© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Introduction to FTTH

© 2009 Cisco Systems, Inc. All rights reserved.

FTTH Motivations/Drivers

- The need for speed!
  - Bandwidth requirements driven by NGN applications
  - Video (HD is a key driver)
  - On demand BW services
- Need for a first mile
  - Availability of Local Loop Unbundling
  - Dependency on Local Loop Unbundling
  - Greenfield Areas
- Streamlining the Access Network
  - Consolidation of Access networks
- Competitive Threat
  - From cable companies & DOCSIS 3.0/Wideband DOCSIS
  - SP's offering FTTH services

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

FTTH The Way to Provide True High Speed Access

- ADSL is reaching it's limitations
- The two major constraints inherent in ADSL technologies,
  asymmetry and bandwidth limitation,
  prevent operators from being able to supply the applications that digital homes will be demanding in the not too distant future.

  With increased penetration download speeds beyond 1.5 to 2 km drops dramatically and the minimum 10Mbps for 3Play (SDTV) cannot longer be provided

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

FTTH Enables New Service Delivery Models

- "Classic" Model: SP provides access and services

  Monopolization of Services, Success depends heavily on innovative services of the SP

- Open Access Model: "Pooling of talents"

  Layered Model, different providers for access and services

  Leveraging strength of individual partners

  Creates platform for new, innovative services

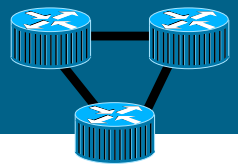
© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

OAN Example:Citynet Amsterdam

Public Orchestrated Open Access Model

ACCESS, SERVICES AND CONTENT

NETWORK (Backbone and Access)



PHYSICAL INFRASTRUCTURE (Dark Fiber)

Multiple Content & Service Providers

BBned (Telecom Italia)

Glasvezelnet (Fibernet) Amsterdam BV

5 Housing Corporations (33,3 %)

Municipality Amsterdam (33,3 %)

ING Real Estate (33,3 %)

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

What Is an Open Access Network

- Provides access on equal terms to Subscriber Service Providers (SSPs)
  - ISPs
  - Voice SPs
  - Video SPs
  - Application SPs

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Requirements for OANs

- Freedom of choice for services: voice, video, data
- Separate billing
- Multiple different SSPs at same UNI
- Security
- Separate authentication
- IP addresses out of SSP’s address range
- Potentially common CPE for multiple services
- Address efficiency
- Scalability
- Traffic segregation

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Reasons for Open Access Networks

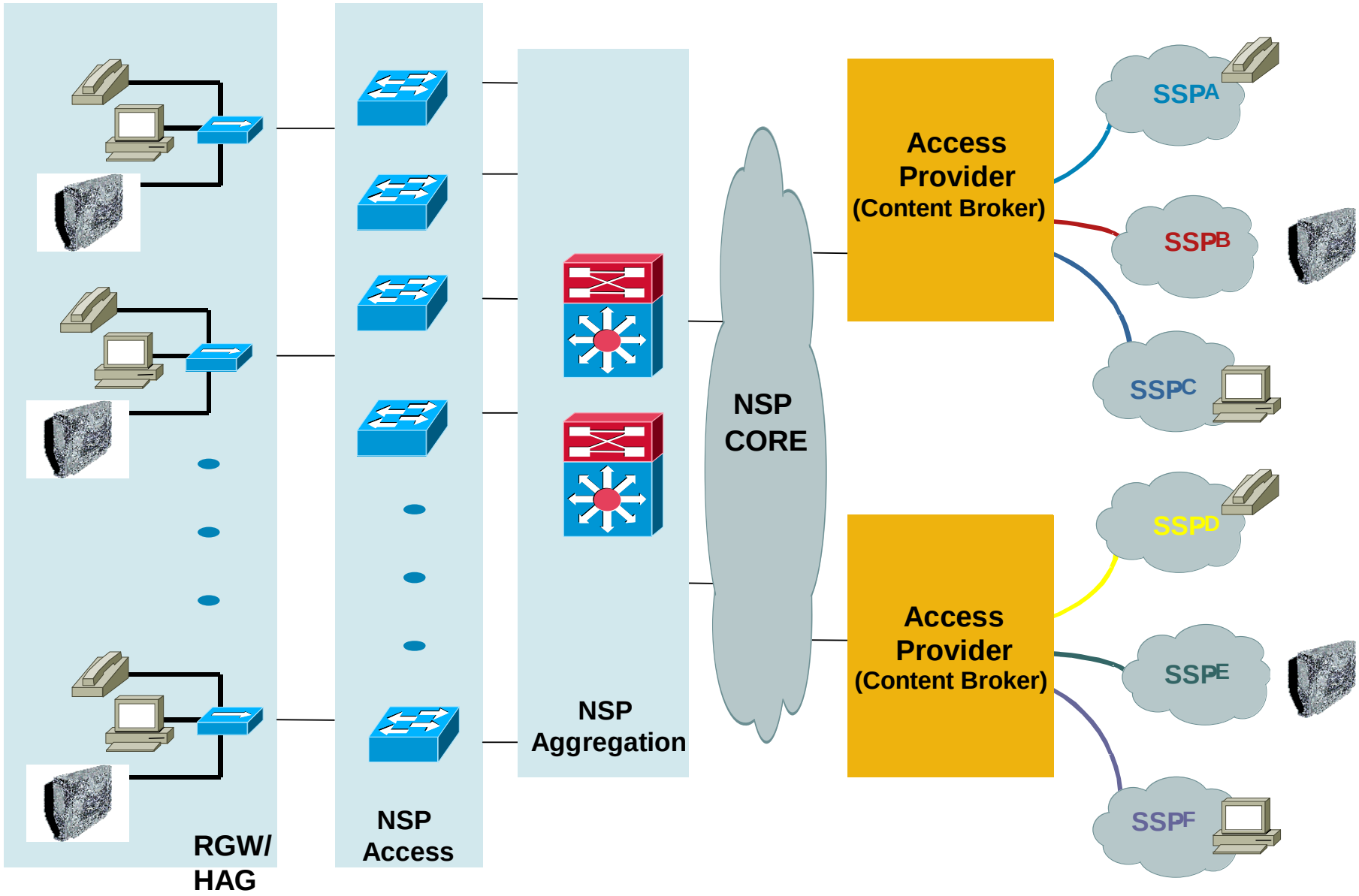
- Future EU regulation (not yet)
- New business model for utilities, real estate companies and municipalities

  Different depreciation cycles for passive and active infrastructure

  Skill sets for digging fibre, operating a telecommunication network and providing services are different

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

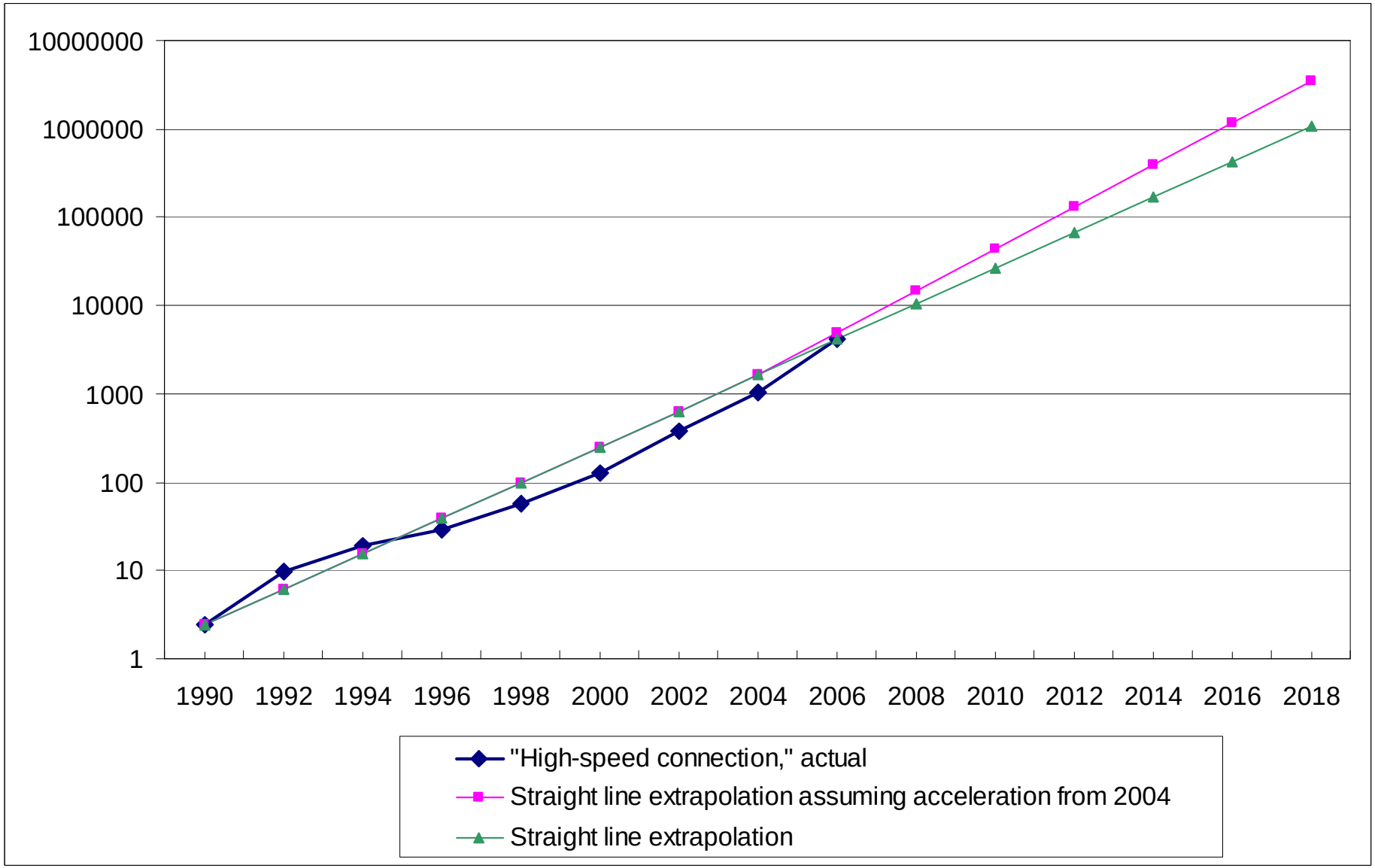
Generic EAN Model



© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

FTTH Infrastructure Is A Long-Term Investment

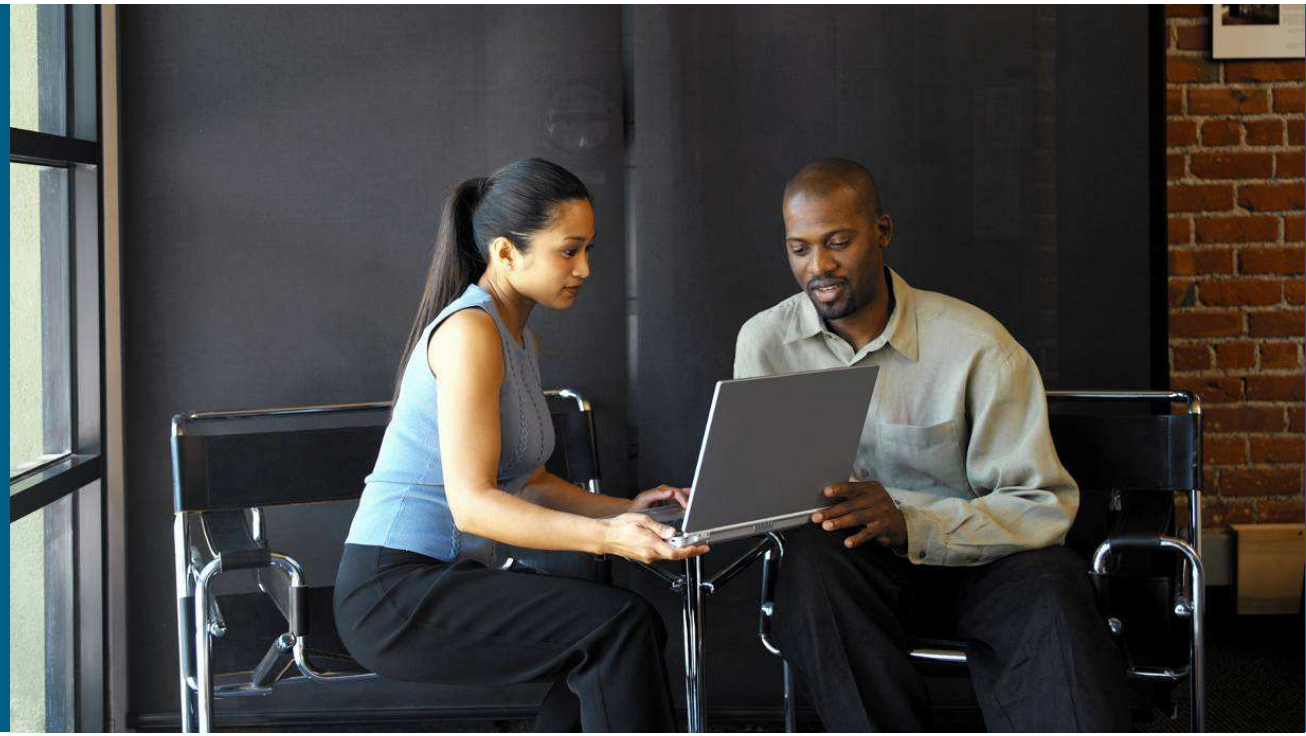
Need To Accommodate Present & Future BW Requirements



Source: Heavy Reading report “FTTH Worldwide Market & Technology Forecast, 2006-2011”

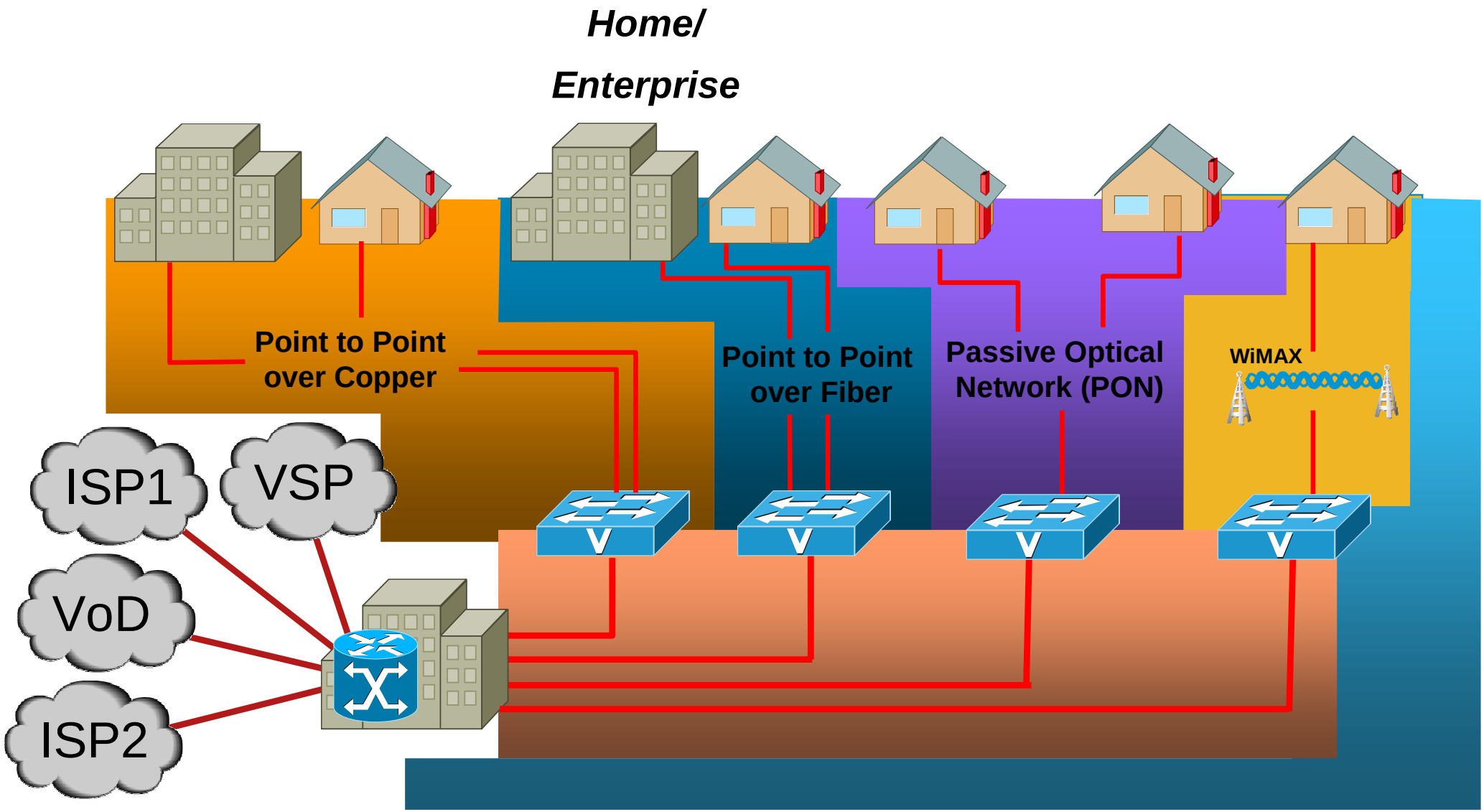
© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

FTTH Technologies



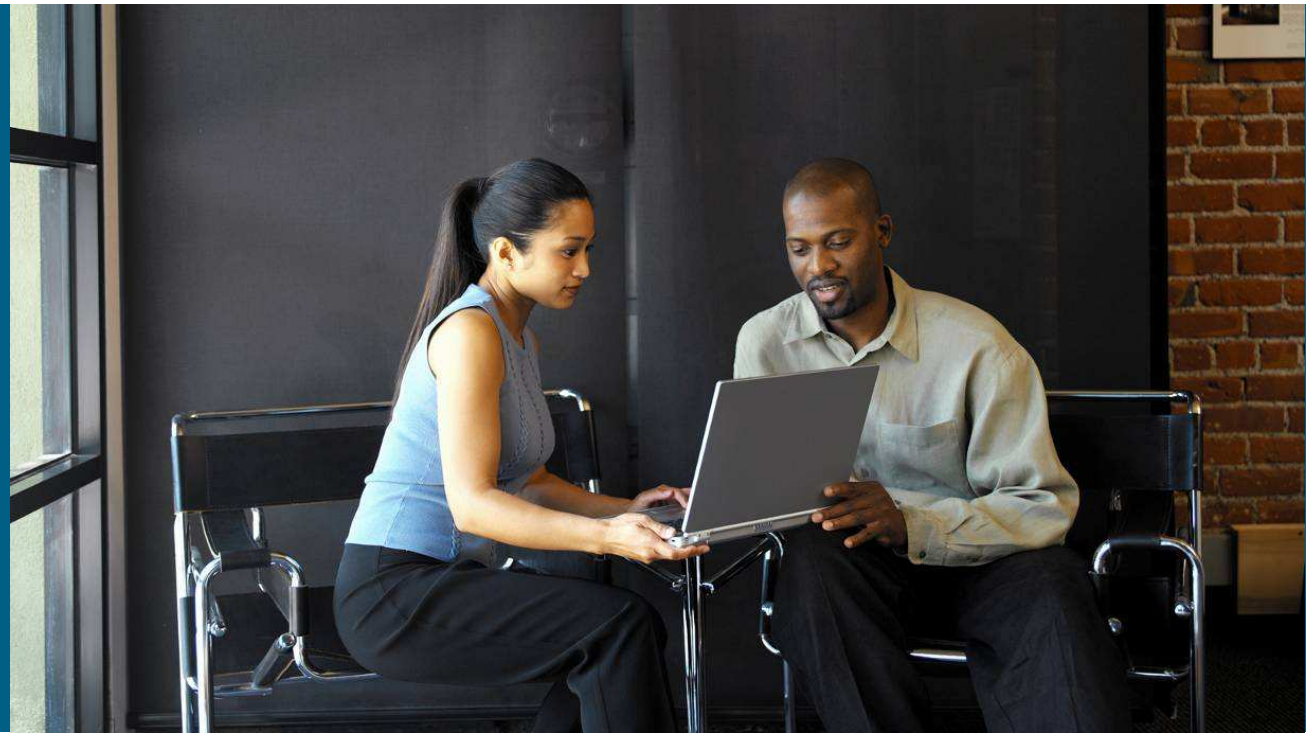
© 2009 Cisco Systems, Inc. All rights reserved.
Cisco Public

Next Generation Network Broadband First Mile Options



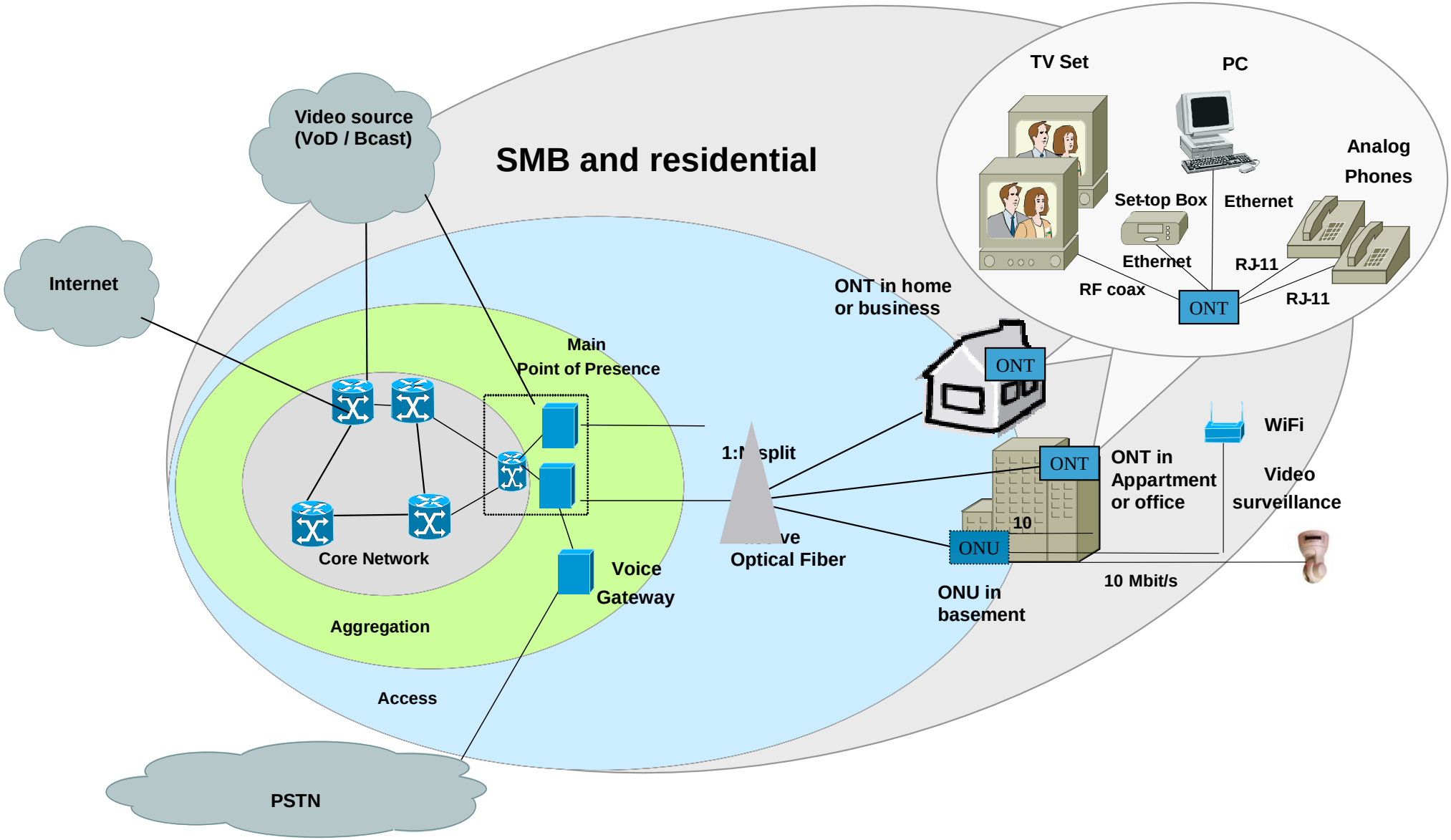
© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Passive Optical Networks



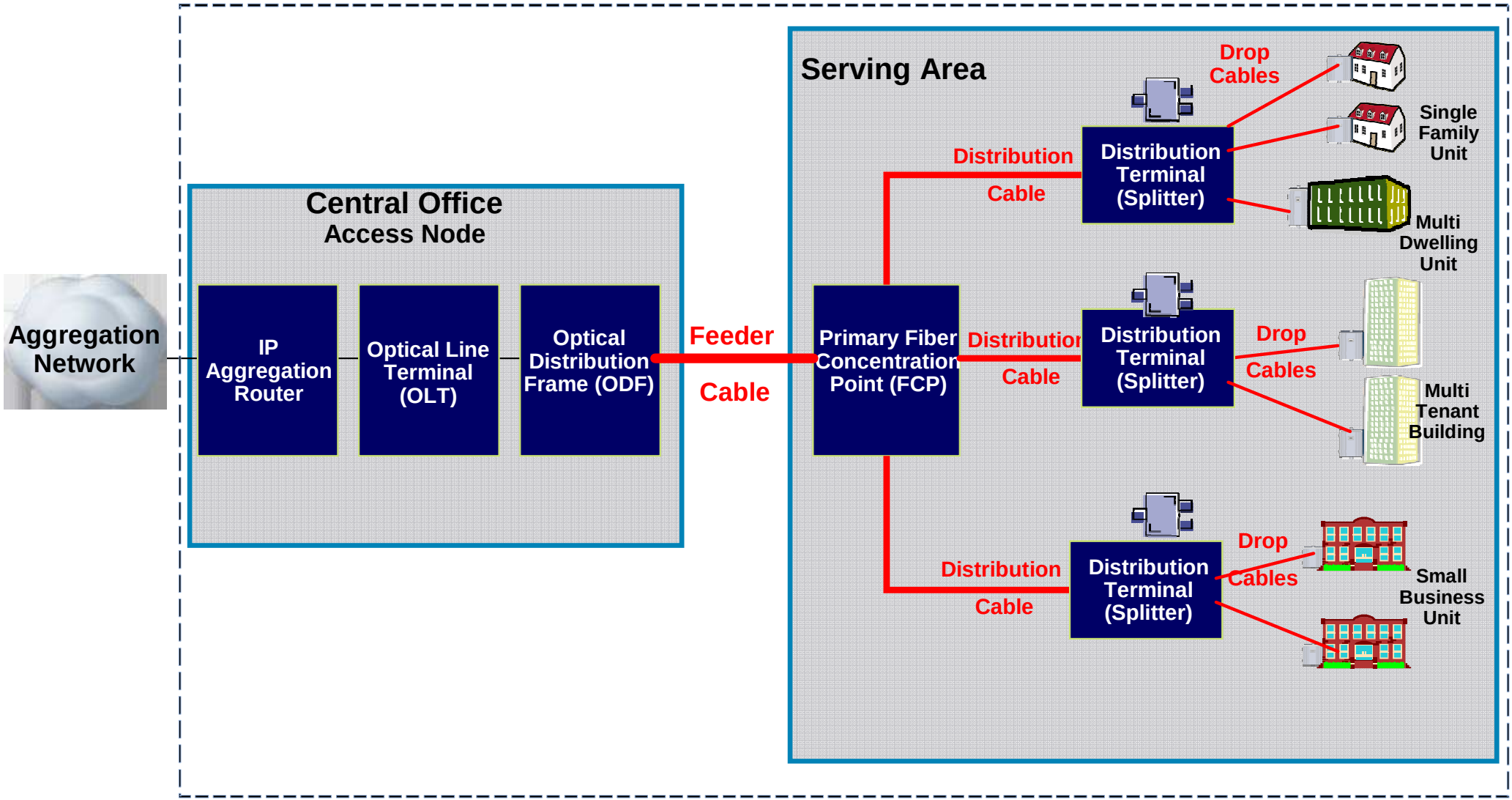
© 2009 Cisco Systems, Inc. All rights reserved.

PON Architecture



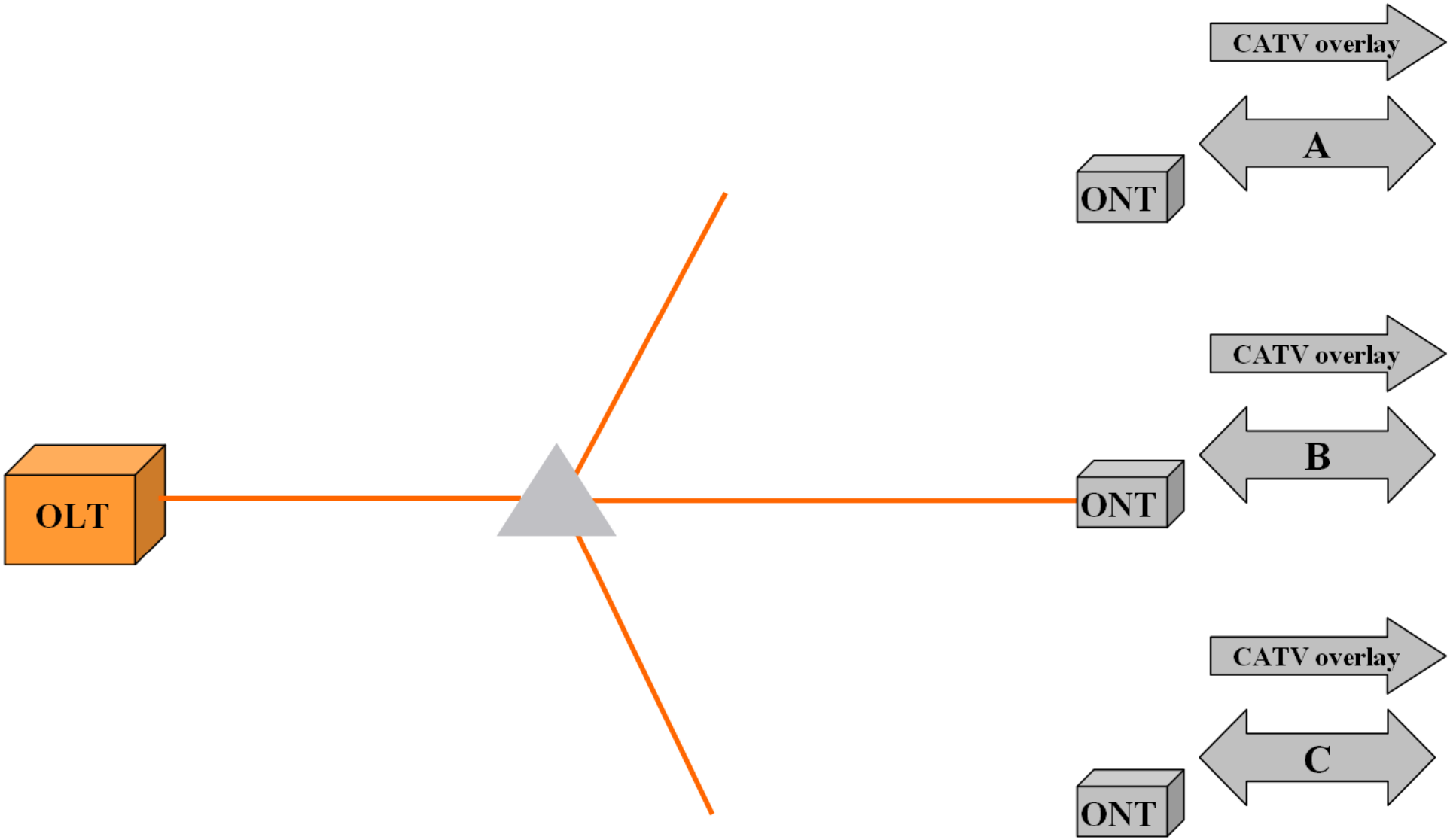
© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

PON Physical Network Infrastructure



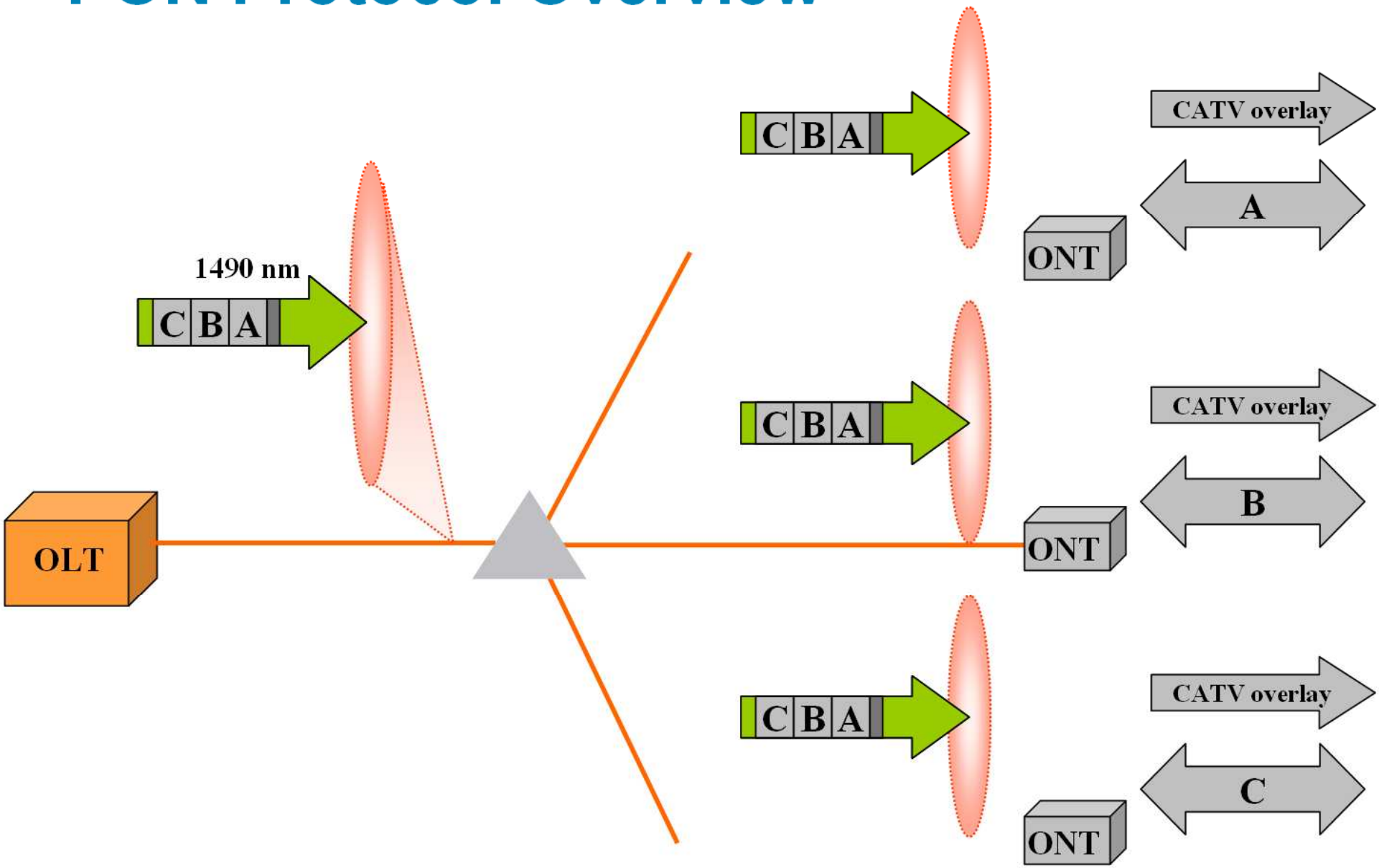
© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

PON Protocol Overview



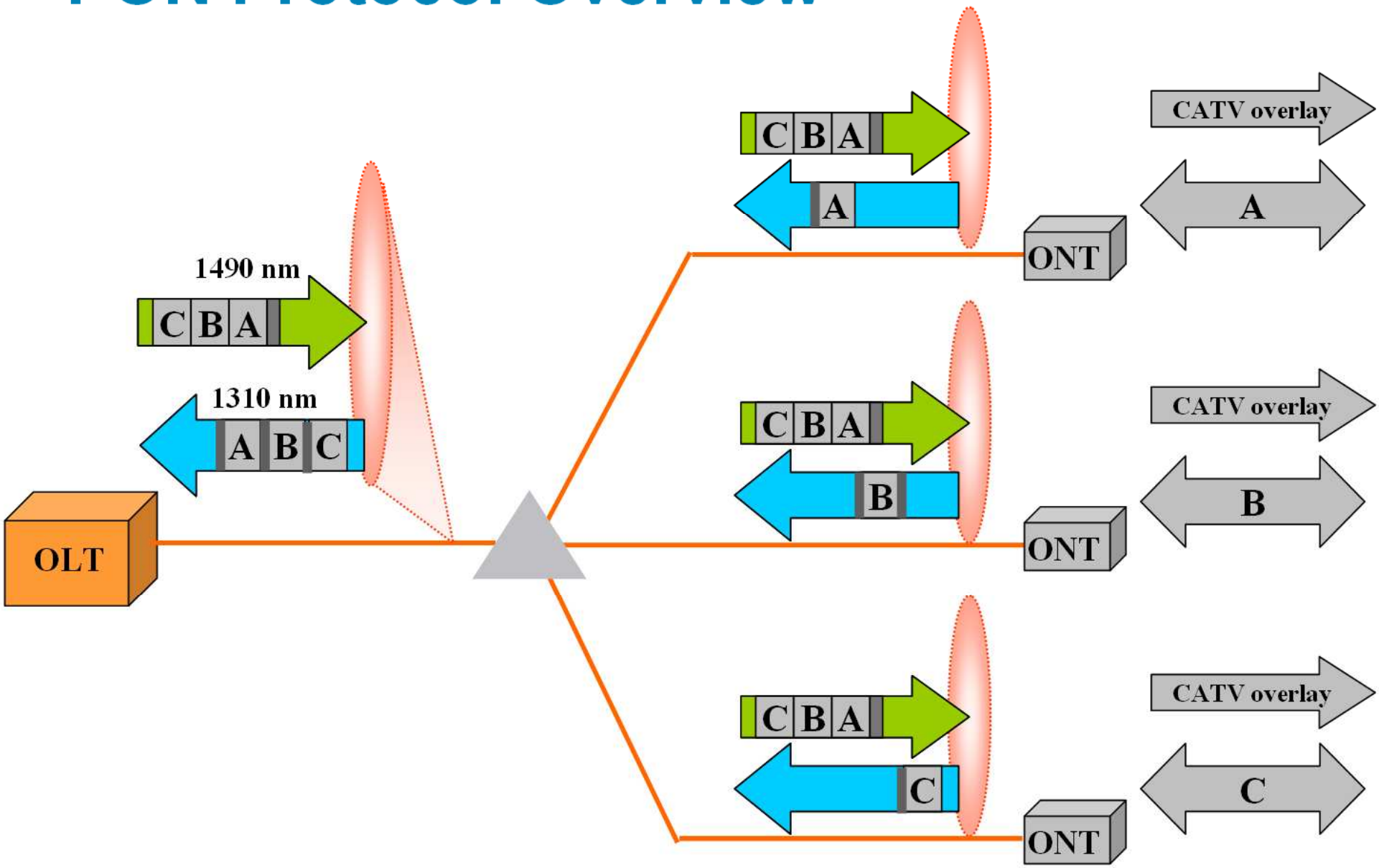
© 2009 Cisco Systems, Inc. All rights reserved.

PON Protocol Overview



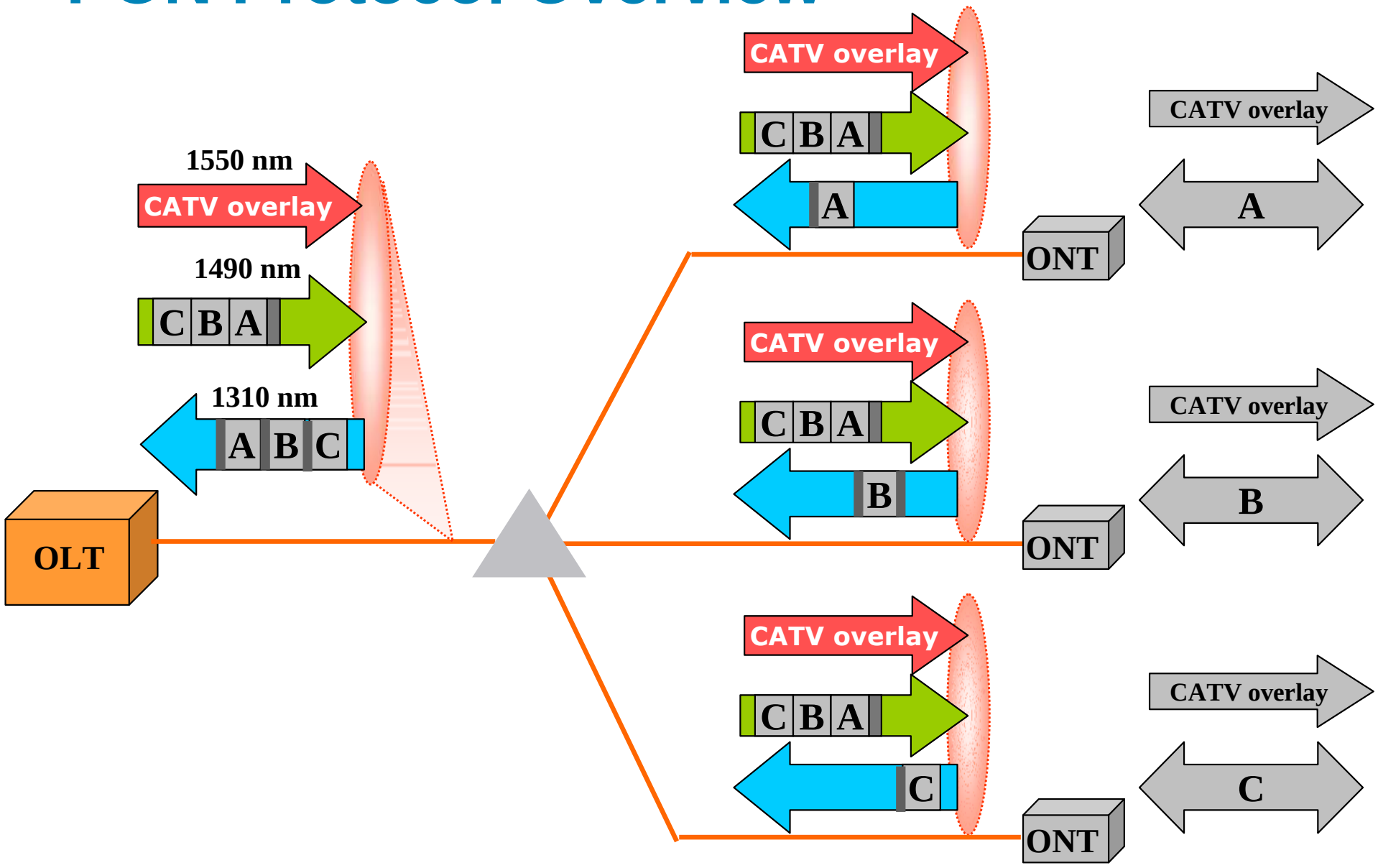
© 2009 Cisco Systems, Inc. All rights reserved.

PON Protocol Overview



© 2009 Cisco Systems, Inc. All rights reserved.
Cisco Public

PON Protocol Overview



© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

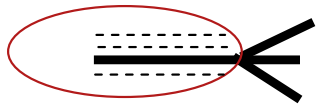
PON Flavors

	BPON	EPON	GPON
Standard	ITU-T G.983	IEEE 802.3ah	ITU-T G.984
Bandwidth	Downstream up to 622 Mbit/s Upstream 155 Mbit/s	Up to symmetric 1.25 Gbit/s	Downstream up to 2.5 Gbit/s Upstream up to 1.25 Gbit/s
Downstream λ (nm)	1490 and 1550	1550	1490 and 1550
Upstream λ (nm)	1310	1310	1310
Transmission	ATM	Ethernet	Ethernet, ATM, TDM

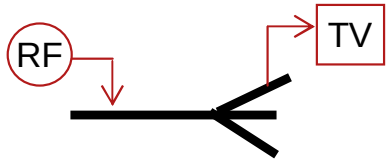
© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Motivations for PON deployment

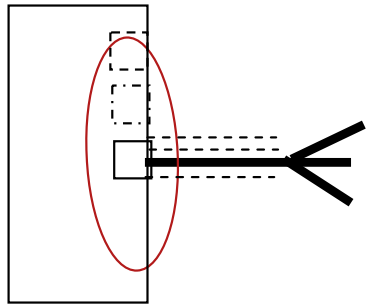
- **Fiber saving between splitter and CO/POP**
  - relevant in scenarios where existing cables or ducts need to be reused towards the splitter, or where fiber deployment is restricted (e.g., aerial cabling)
  - Less relevant for Greenfield scenarios (marginal cost of fiber compared to digging, splicing, ...)



- **Analog video overlay for existing broadcast services**
  - emulates cable TV distribution plant on a separate downstream wavelength delaying introduction of IP TV
  - requires equivalent of cable headend at each OLT side



- **Port saving in the CO/POP**
  - need to terminate thousands of fibers on switch ports
  - PON can reduce this by 1...2 orders of magnitude compared to P2P
  - port costs on a per-customer base, however, are roughly equivalent



- **No deployment of active equipment in the outside plant**
  - in Europe & Middle East typically loops are sufficiently short
  - so that P2P deployments do not require active equipment in the outside plants

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

About Next-Gen PON: GPON vendors say ...

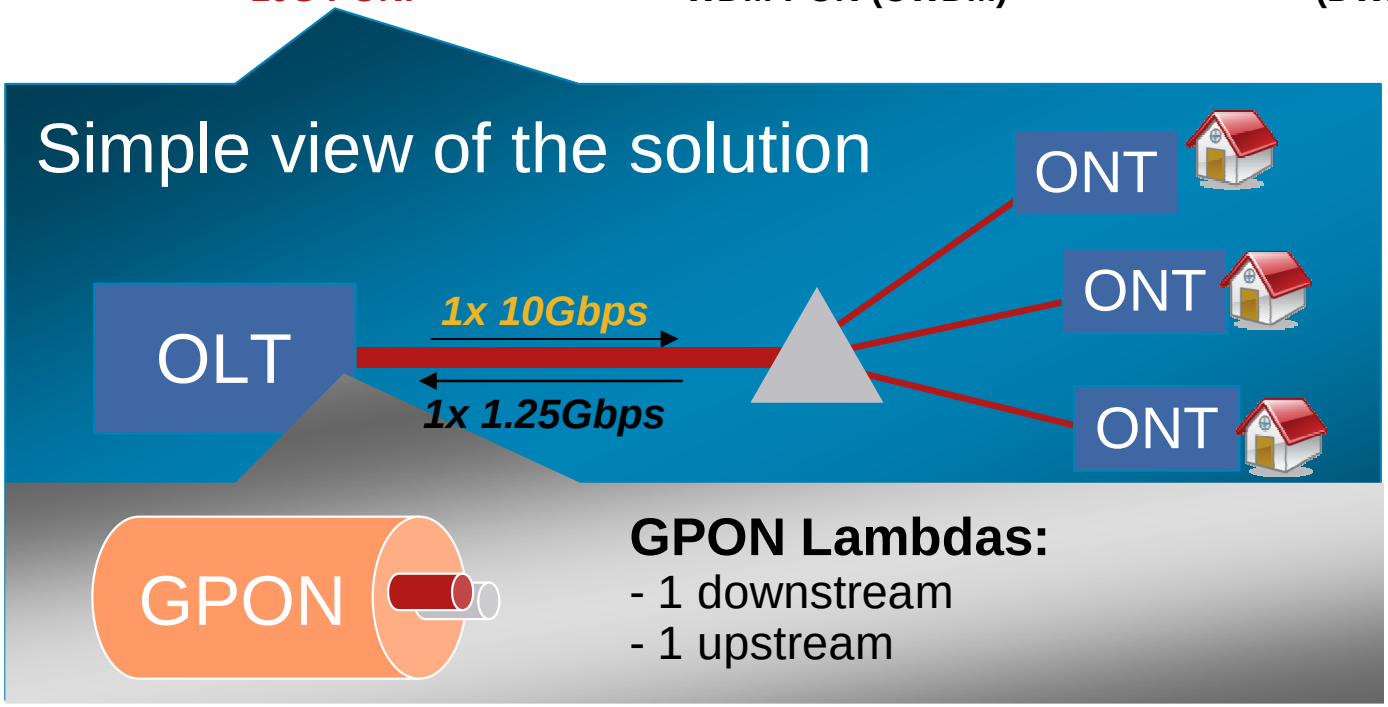
2006	2009	2010	2011+
GPON up and running.	More bandwidth. New optical components. 10G PON.	More capacity with Wavelenght multiplexing. WDM-PON (CWDM)	More capacity and bandwidth with One wavelength per subscriber. (DWDM)

None of this is standardized yet…

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

About Next-Gen PON: GPON vendors say ...

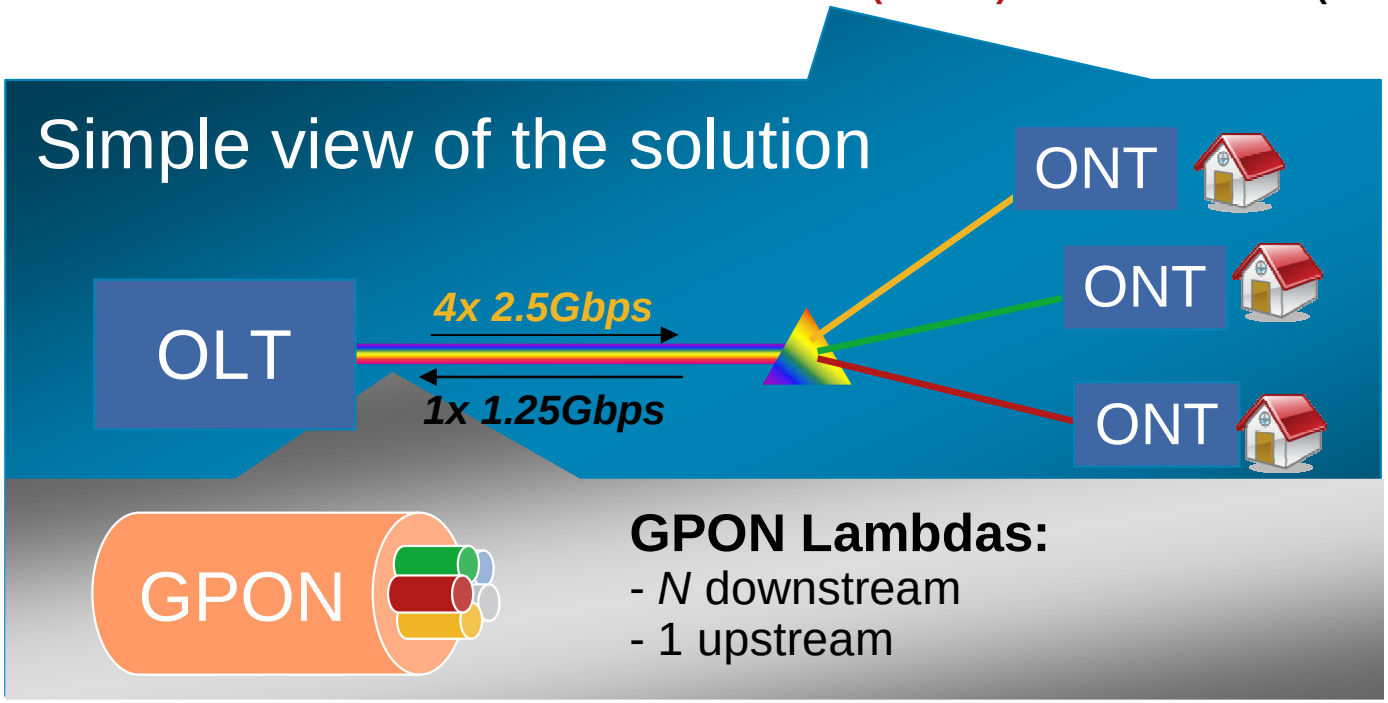
2006	2009	2010	2011+
GPON up and running.	More bandwidth. New optical components. 10G PON.	More capacity with Wavelenght multiplexing. WDM-PON (CWDM)	More capacity and bandwidth with One wavelength per subscriber. (DWDM)



© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

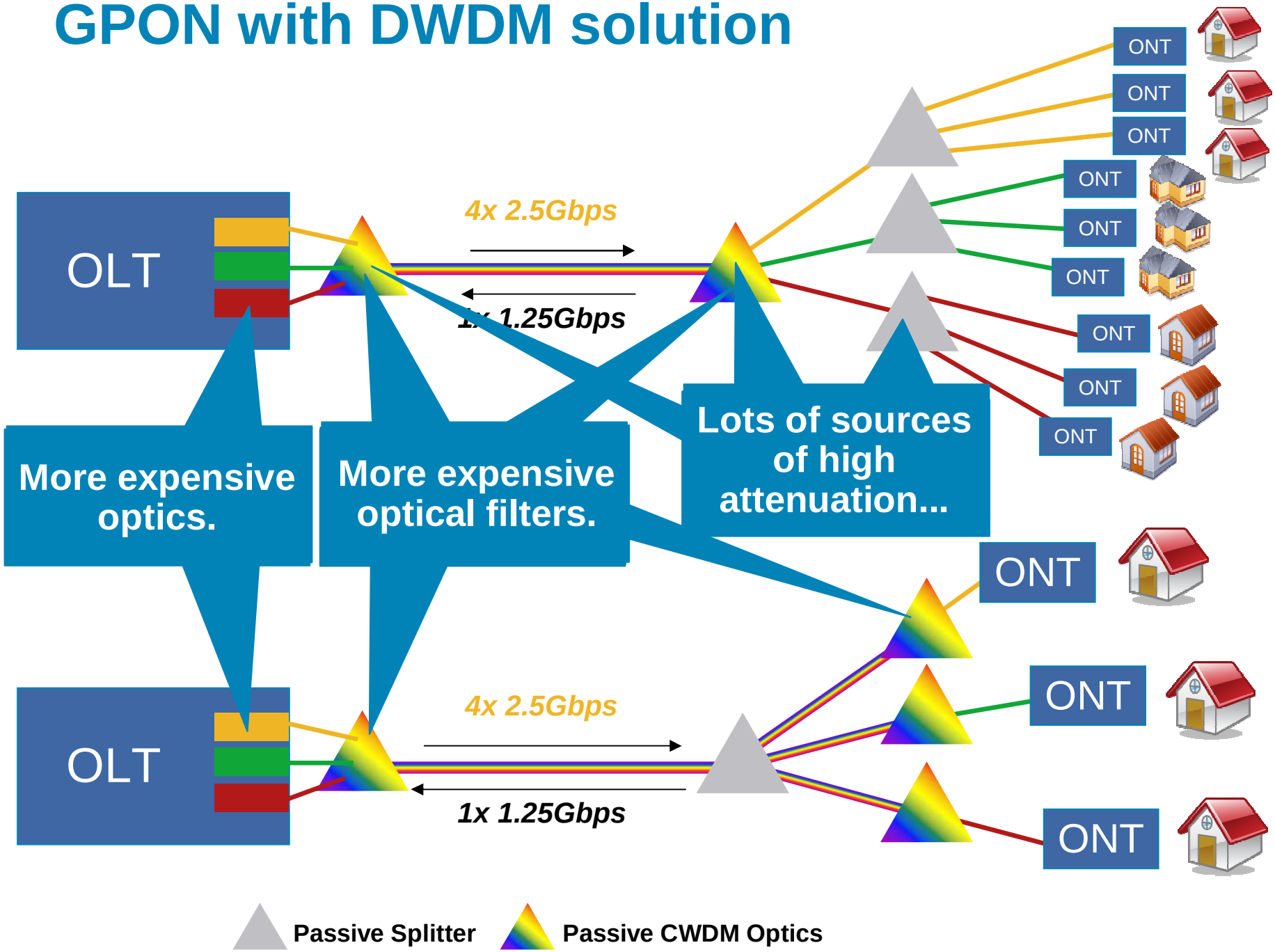
GPON vendors say ...

2006	2009	2010	2011+
GPON up and running.	More bandwidth. New optical components. 10G PON.	More capacity with Wavelenght multiplexing. WDM-PON (DWDM)	More capacity and bandwidth with One wavelength per subscriber. (DWDM)



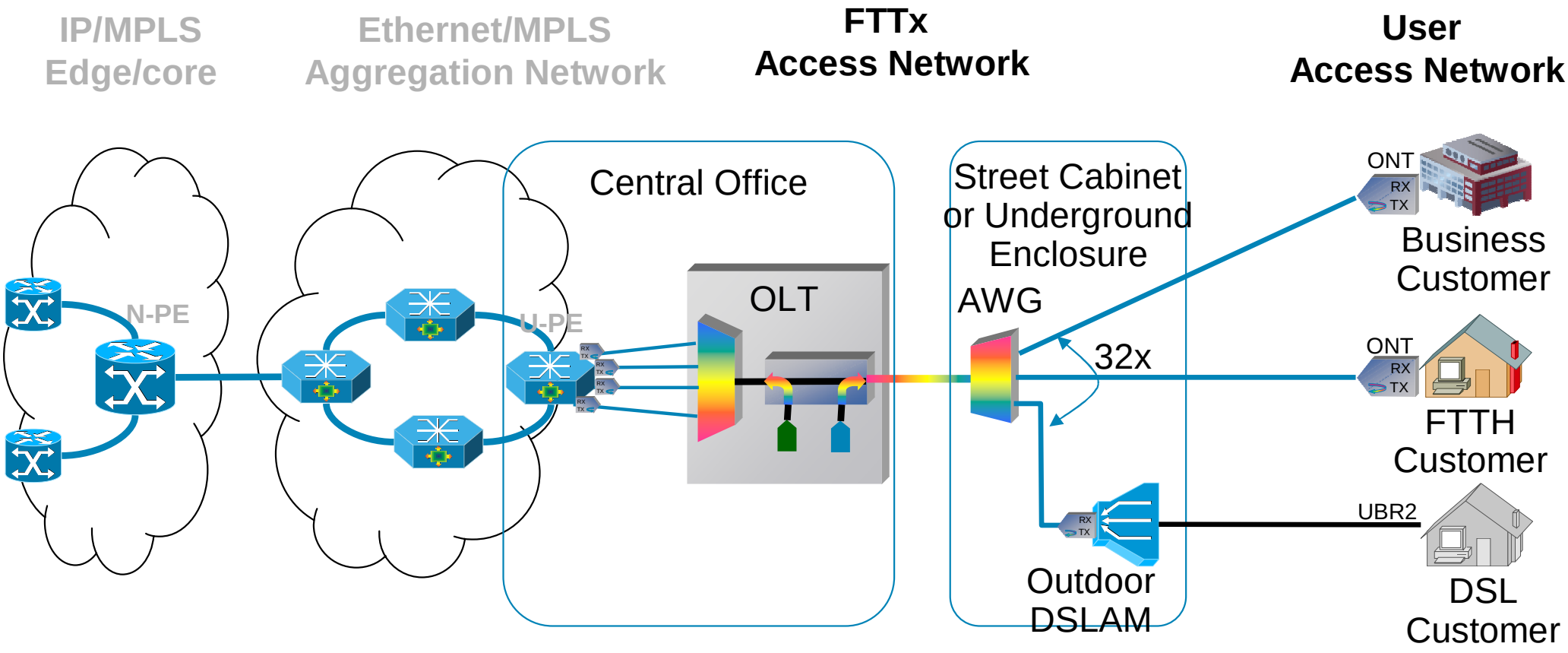
© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

A more realistic way of viewing the GPON with DWDM solution



© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

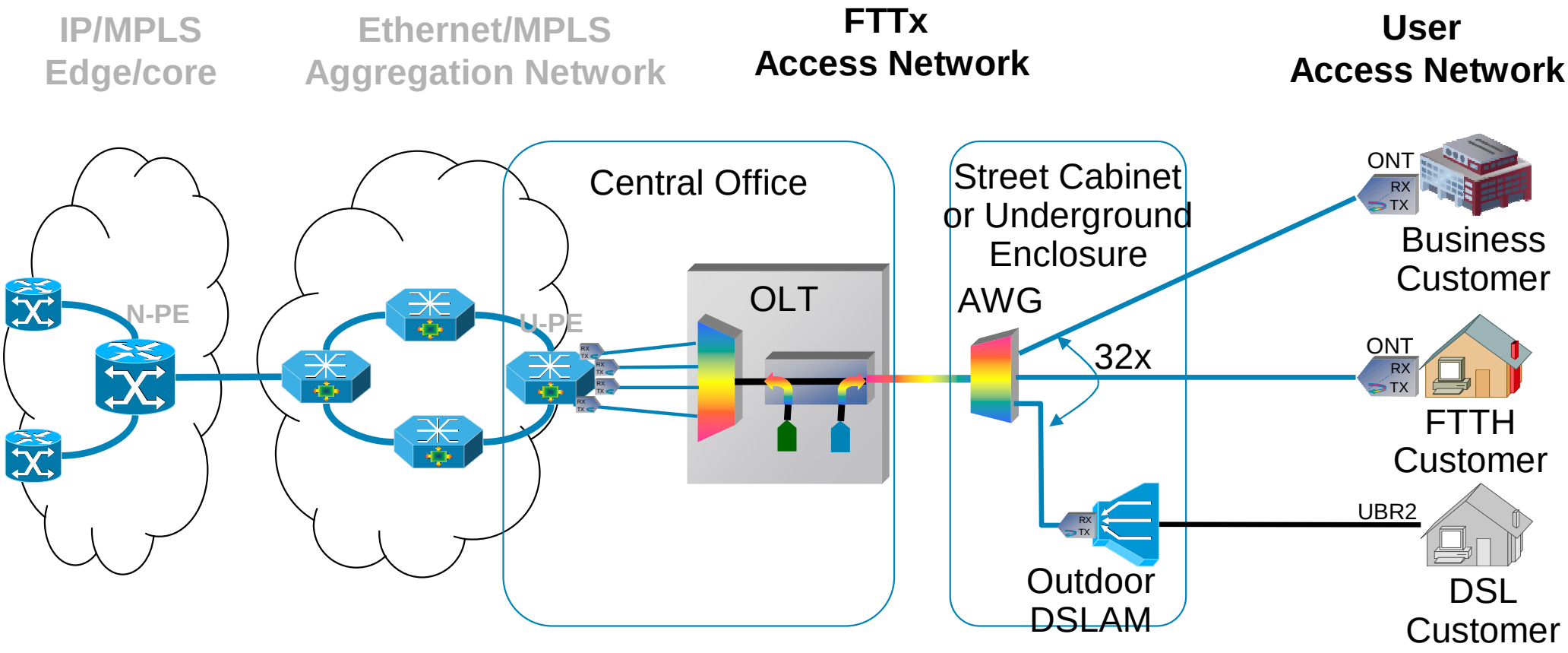
DWDM PON Architecture



- Single feeder fiber from CO to remote node
  => duct space needs similar to GPON
- Single drop fiber per subscriber from the remote node

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

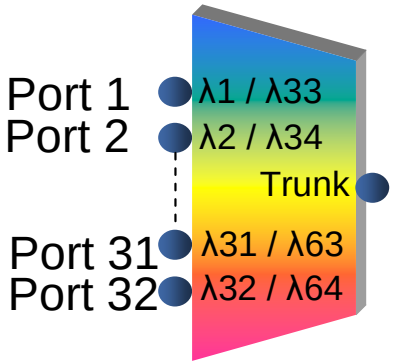
DWDM PON Architecture



- Two dedicated wavelengths, according to ITU-T 100GHz grid, per user
- Minimized component diversity (same optics for every end point)
- Flexibility for ONT/ONU (managed, unmanaged, switch, router)

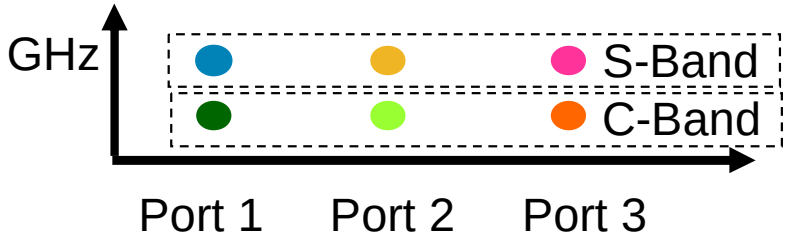
© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Components of DWDM PON Solution



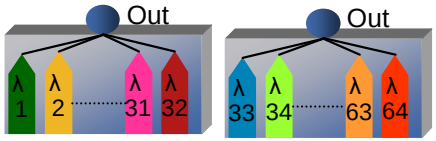
AWG: **A**rrayed-**W**aveguide **G**rating

- Periodic filter characteristic: two bands per port (S- and C-Band)
- Fan-out 1/32 (32 upstream and downstream wavelengths)



4 - Port Optical Circulator

- Insertion of directed injection light



Laser Arrays

- Generate the spectrum of injection wavelengths

Transceiver:

- Receiver and transmitter in one SFP per fiber
- Receiver: wavelength agnostic
- Transmitter: **R**eflective **S**emiconductor **O**ptical **A**mplifier

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Main Issues with PONs

- **Data sent to all users on the tree: inefficient Video multicast & VoD**

  IGMP Proxy and snooping with limited support. IGMP process distributed between OLT(Proxy) and ONT(Snooper) instable. Zapping degrades with large number of channels selected. No state of IGMP on ONT kept. Troubleshooting by “mirroring” PONT tree, no focus on one sub (trace per user) possible Asymmetrical

- **Strong encryption required to prevent eavesdropping**
- **No resilience**

  –OLT optics is single point of failure for entire tree

  –corrupt CPE can impact entire PON tree

- **Jamming is very easy**

  –just transmit continuous light and the whole tree is OOS

- **In case of technology change all terminations on a tree need to be replaced (simultaneously?)**
- **Every endpoint (OLT, ONT, ...) has to operate at the aggregate bitrate**

  –e.g., a GPON ONT delivering 100 Mbit/s to an end customer has to operate at 2.5 Gbit/s

- **All FTTH deployments that we are aware of universally assume a take rate of 25...35%.**

  –Theoretical maximum number of customers per tree is rarely reached due to take-up rates

  –Only 25-35% of interfaces need to be accommodated on switches in a Eth. P2P scenario rather than 100% in PON

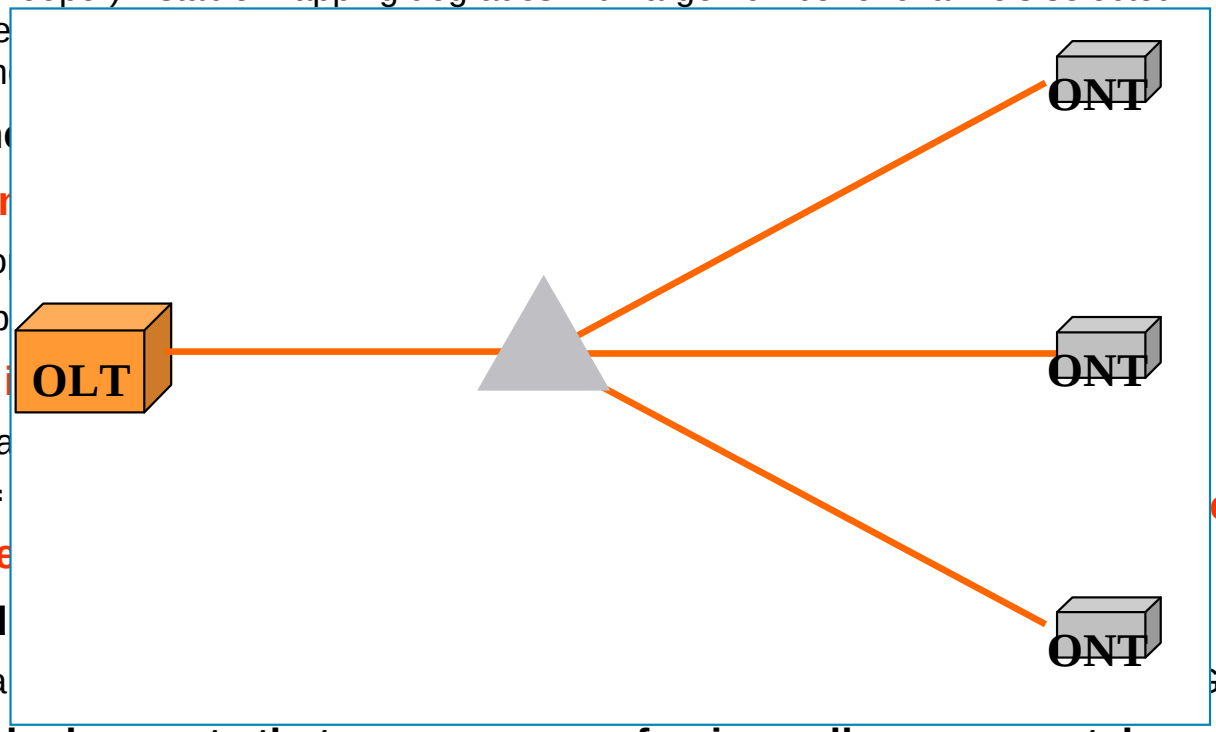
© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Main Issues with PONs

- **Data sent to all users on the tree:** **inefficient Video multicast & VoD**

  IGMP Proxy and snooping with limited support. IGMP process distributed between OLT(Proxy) and ONT(Snooper) instable. Zapping degrades with large number of channels selected. No state of IGMP on ONT ke… user) possible
  Asymm…

- **Strong en…**
- **No resilien…**
  - –OLT o…
  - –corrup…
- **Jamming i… OLT**
  - –just tra…
- **In case of … ced**
  (simultane…
- **Every end…**
  - –e.g., a… …Gbit/s



- **All FTTH deployments that we are aware of universally assume a take rate of 25...35%.**
  - –Theoretical maximum number of customers per tree is rarely reached due to take-up rates
  - –Only 25-35% of interfaces need to be accommodated on switches in a Eth. P2P scenario rather than 100% in PON

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

PON CPE Aspects

- CPE's (a.k.a. ONU's or ONT's) are an integral part of the PON architecture
- Special functionality
  - Media Access Control
  - Burst-mode lasers
  - High optical power
  - Encryption
  - High speed (needs to support PON line rate)

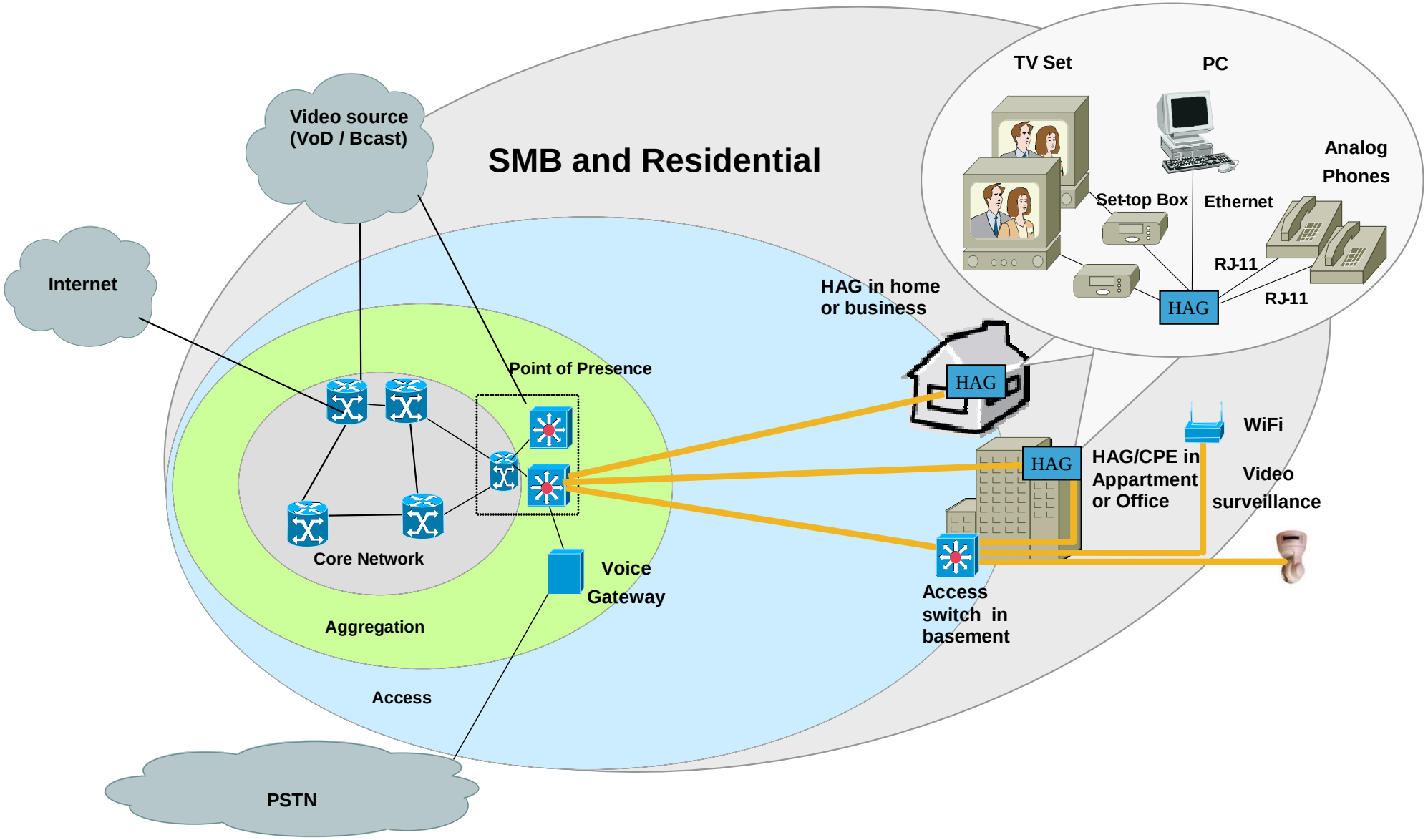
  makes PON-CPE's inherently more expensive than native Ethernet CPE's
- Multi-vendor interoperability left for the future
- Typically deployed and owned by the Service Provider as corrupt CPE's can impact the traffic of other customers and compromise security

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Point-to-Point (P2P) or home run fiber

© 2009 Cisco Systems, Inc. All rights reserved.

Ethernet Star Architecture



© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Ethernet Star Architecture Characteristics (a.k.a. P2P)

- Direct fiber access to individual subscribers (e.g. single family residences, apartments)
  - Access switches in CO or decentralized on customer premise
  - Single mode single fibre
- MTU deployments for residential, SMB, and Enterprise customers
  - Access switches in basement of MTU; last drop via UTP (Cat6/7) or fiber (SM/MM)
- Very flexible and future proof solution as it allows virtually unlimited bandwidth per customer

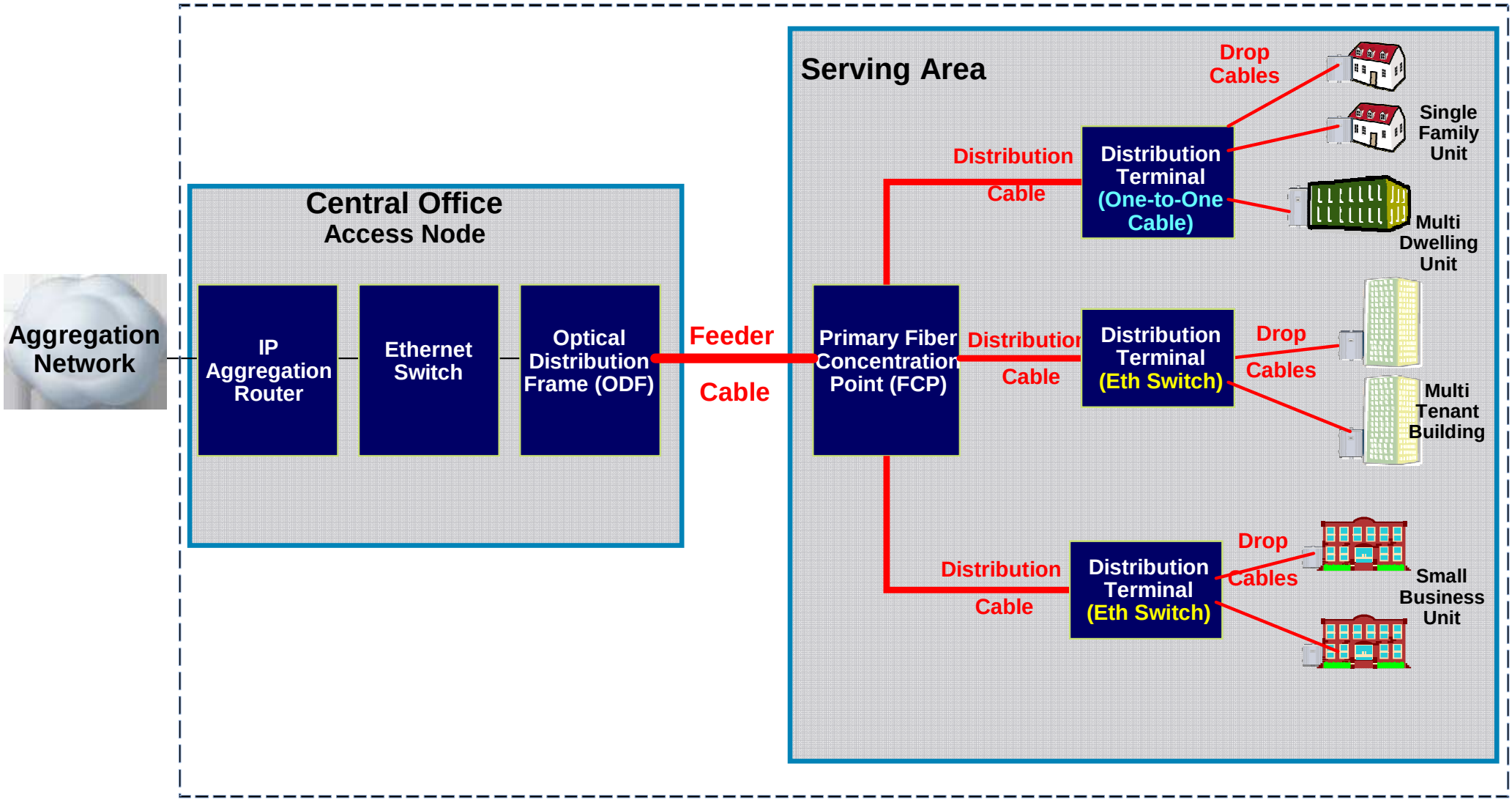
© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Ethernet Star Architecture Characteristics (a.k.a. P2P)

- Pay as you grow possibility
- Fiber topology is technology neutral
- Migration to new technologies / higher speeds can be done on a customer by customer basis (enabling competition among different technologies / speeds)
- Higher number of fibers to CO/POP

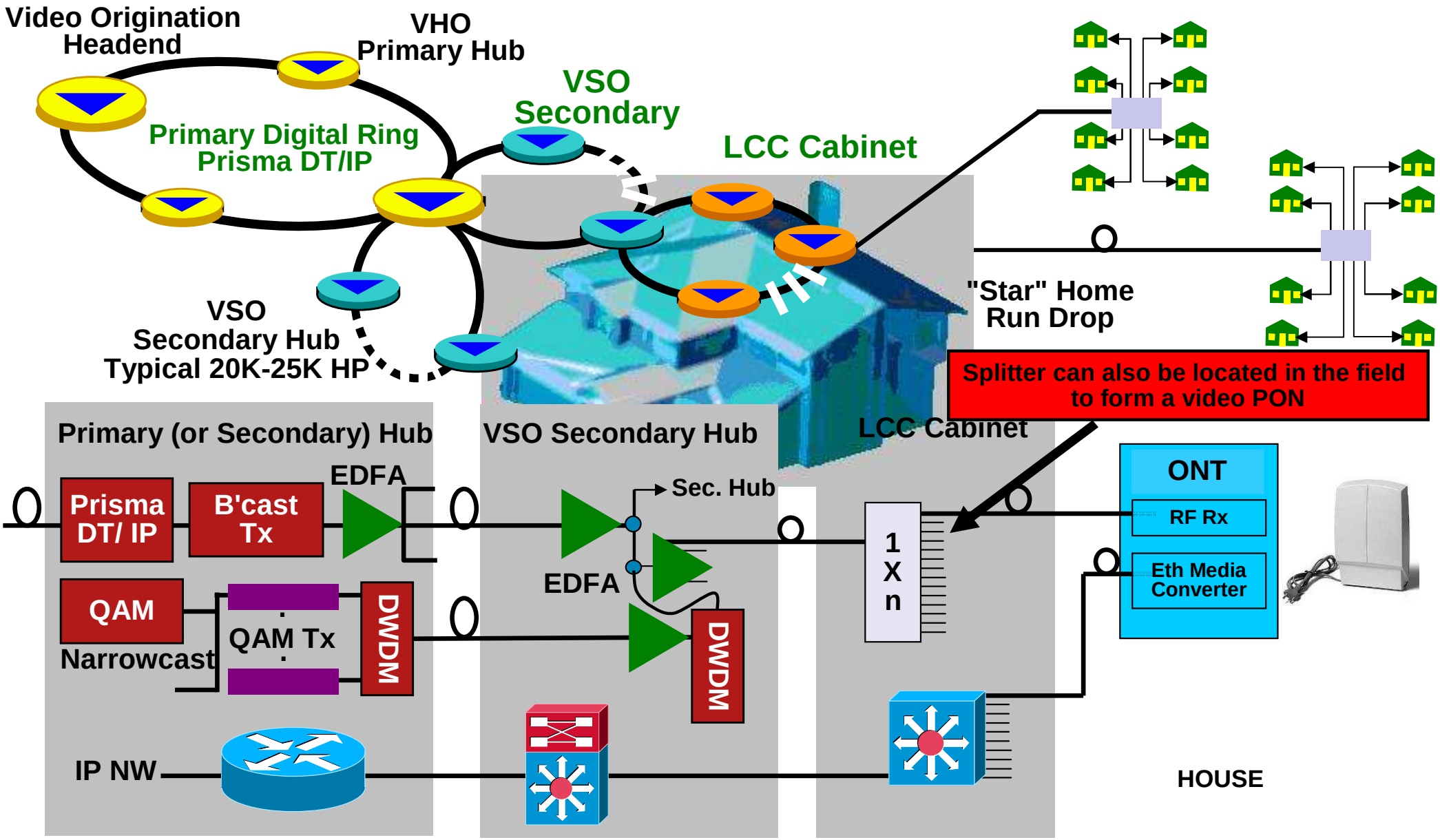
© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Ethernet Physical Network Infrastructure



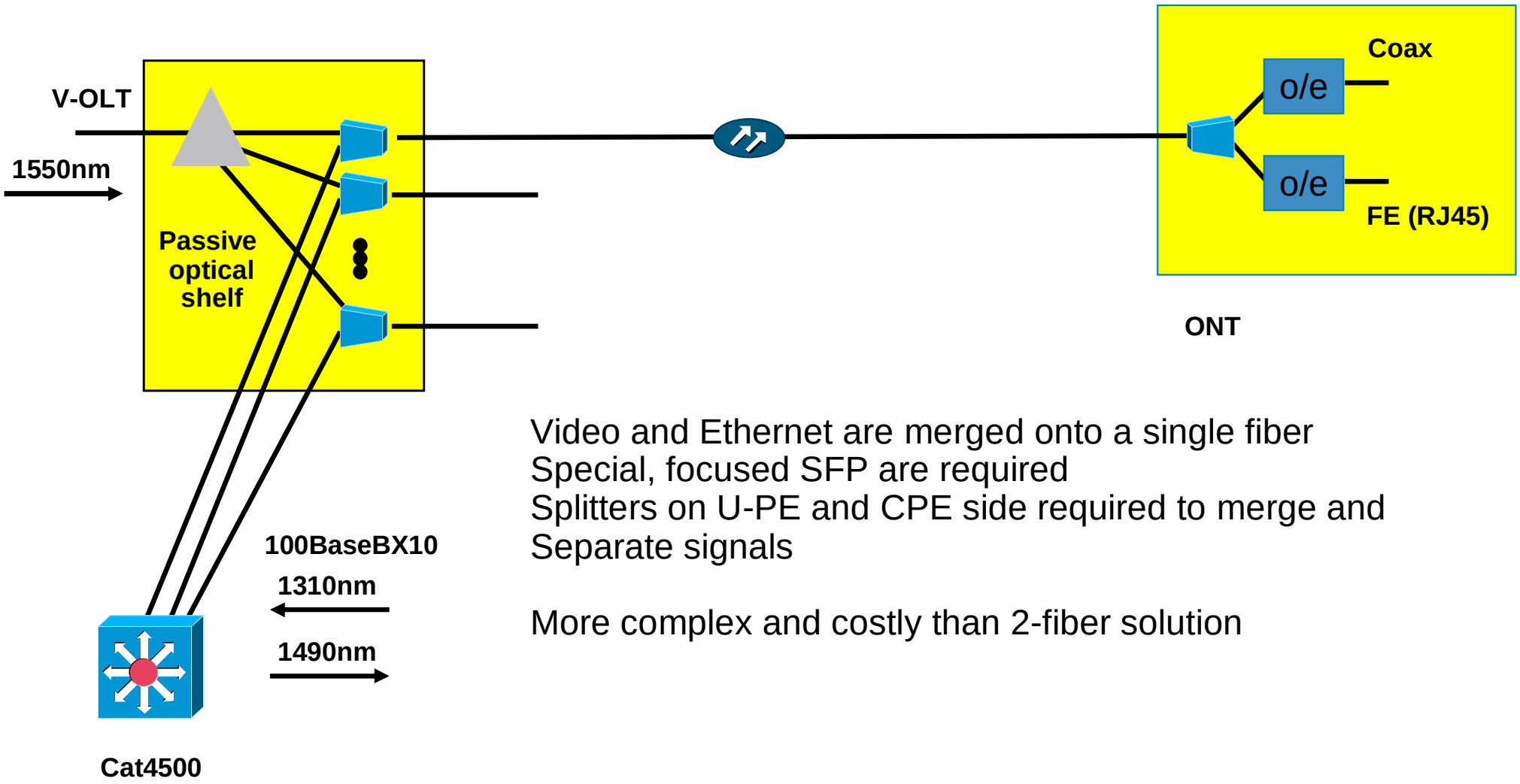
© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Video overlay for P2P Ethernet



© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Single Fiber Video Overlay Concept



Video and Ethernet are merged onto a single fiber
Special, focused SFP are required
Splitters on U-PE and CPE side required to merge and Separate signals

More complex and costly than 2-fiber solution

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

CPE Aspects

- CPEs can be commodity items purchased at retail stores
- No interoperability issues
- No special functionality required
  - No Media Access Control
  - No Burst-mode lasers
- CPE's inherently less expensive than PON CPEs
- Can be deployed and owned by the customer as corrupt CPE's can not impact the traffic of other customers or compromise security
  - just switch off the port in case of non-compliant CPE behavior

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Ethernet Point-to-Point Advantages

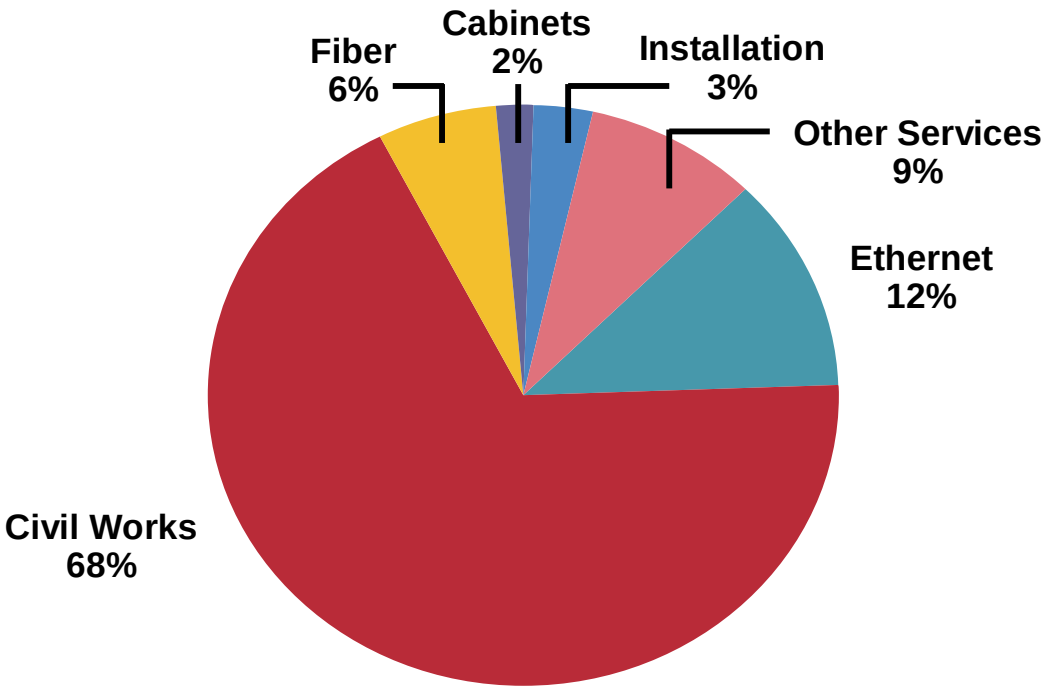
- Dedicated Bandwidth Per User
- Greenfields: Fiber topology is not tailored to- and limited by a given technology
- Ethernet is a commodity
  - Lower port prices
  - Wide interoperability
- Allows cost-effective and still future proof hybrid deployments
  - Mix of Fiber To The Home and Fiber To The Curb with Copper(UTP) connection to the subscriber
- Co-Existence of Business and Residential Subscribers
  - Residential subscribers cannot interfere with business services and SLA's

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

FTTx Deployment

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Cost of Equipment and Construction Deployment models



Source: Corning and FTTH Council Europe

- Civil Works cost is the major share of FTTx deployment and is common to both PON and P2P
- Fiber Cost is only 6% of a FTTx network cost

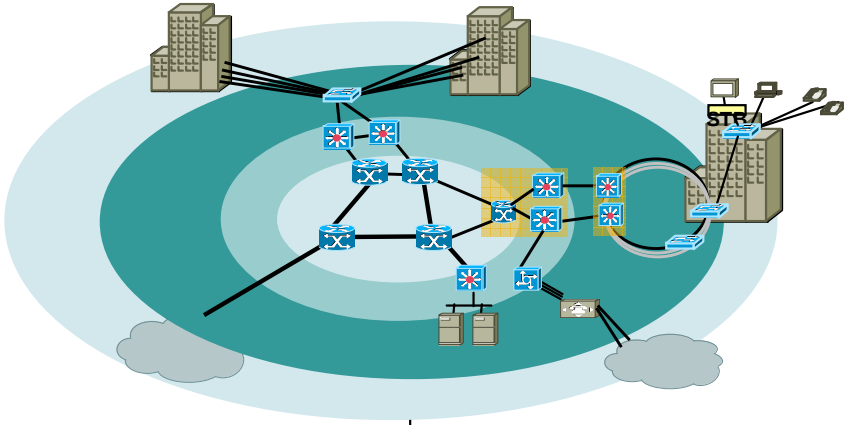
  Fiber lifetime varies between 15 and 25 years

  Increased fiber cost of P2P vs. PON is only a minor part of the overall cost of deployment and has to be regarded in 15-25 years depreciation

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

FTTH Subscriber Connection

FTTH Network



Residential Gateway

Home Network

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

FTTx Point-to-Point
Physical Subscriber Connection

1. New multi/single mode fiber

- ➔ Simple to deploy, Quick User Activation, Unlimited Bandwidth, Easy upgrade to GE access
- ➔ Multimode up to 500m, for in-building wiring
- ➔ Singlemode-single fiber for 100Mb/s and 1000Mb/s up to 10km
- ➔ Quick Installation in existing risers (no safety/interference issues)

2. UTP Copper CAT V-VII

- ➔ In New Buildings (dedicated ducts) Installation quicker and simpler than fiber
- ➔ Network Components (U-PE & CPE) have lower cost than fiber equivalent
- ➔ Future Proof Media for Speeds Up to 1Gb/s
- ➔ Limited to 90m of distance (100m including patching)

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

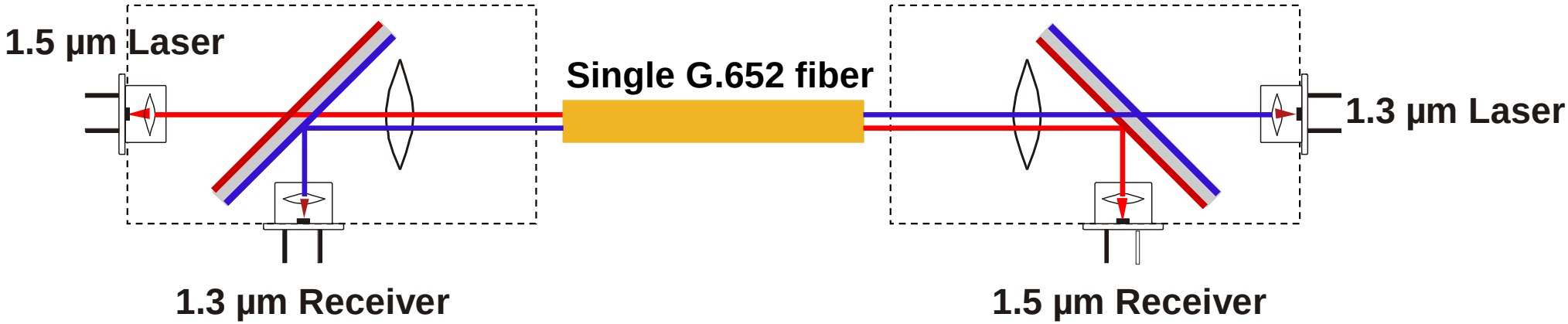
IEEE 802.3ah Ethernet First Mile 100/1000MB/s Interface Definitions

- 100BaseLX-10

  100 Mb/s Interface, up to 10km over Dual Single Mode Fiber

- 100BaseBX-10 (1000BaseBX-10 for GE)

  Single Fiber Connectivity up to 10km over Single Mode Fiber



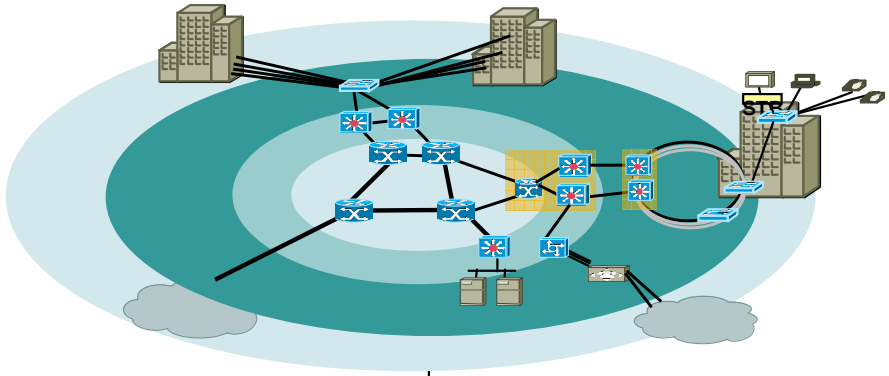
Principle of a 2 Wavelength Device

Laser and receiver in the same package where optical light path is split into second and third window by a WDM filter.

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Customer Premises Equipment

FTTH Network



Residential Gateway

Gaming

TV Service

Voice and Fax Service

Internet Service

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Customer Premise Equipment

- SP's regard the CPE as demarcation point for the service and termination of the FTTH line
- 2 types of CPE approaches, depending on the service offering
- ONT (Optical Network Termination)

  Terminates incoming fiber and converts 100/1000BaseFX/BX/LX10 to 100BaseT

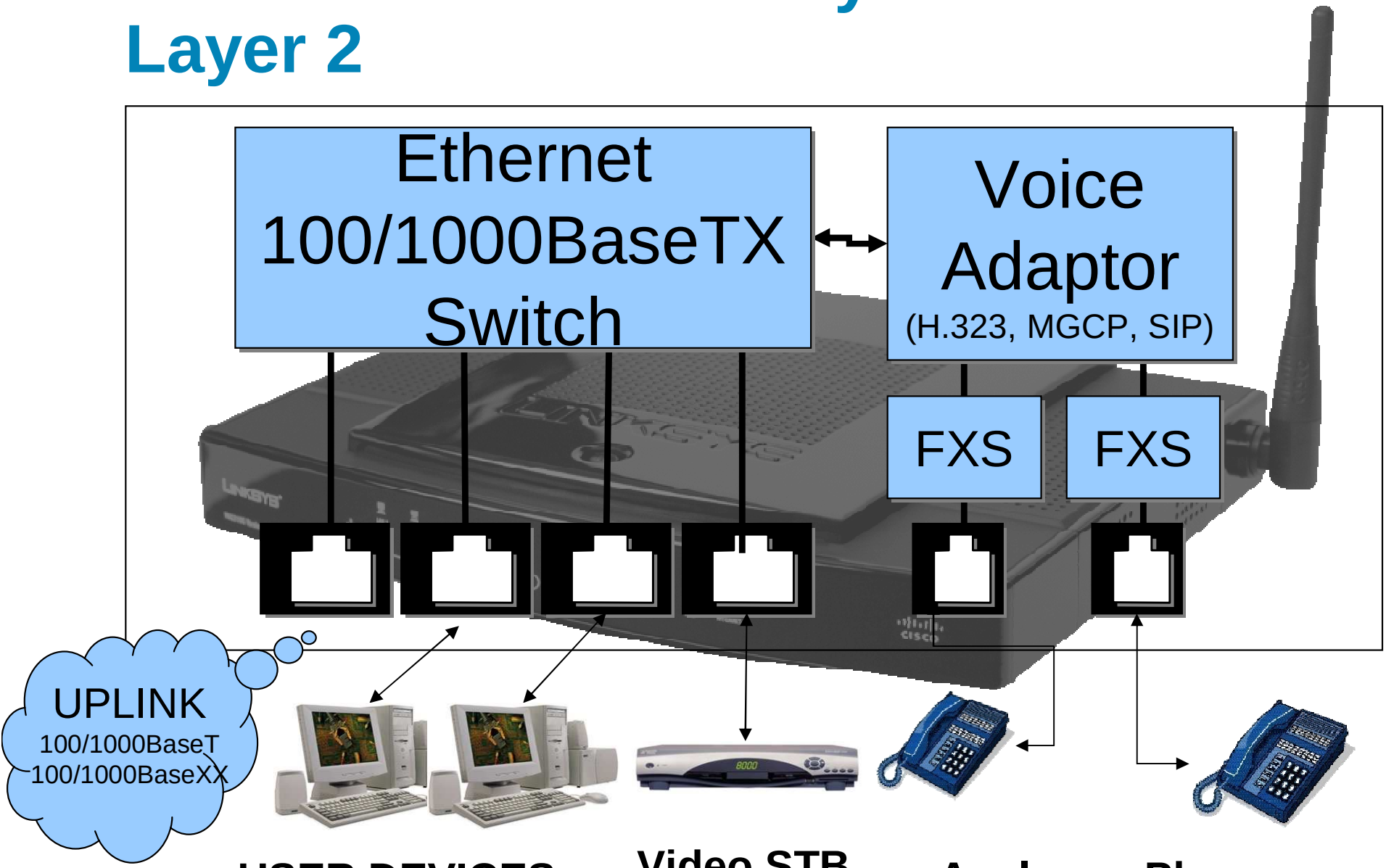
  Customer connection via UTP
- HAG (Home Access Gateway)

  Combined ONT and Service termination

  Mostly Voice/Data combinations

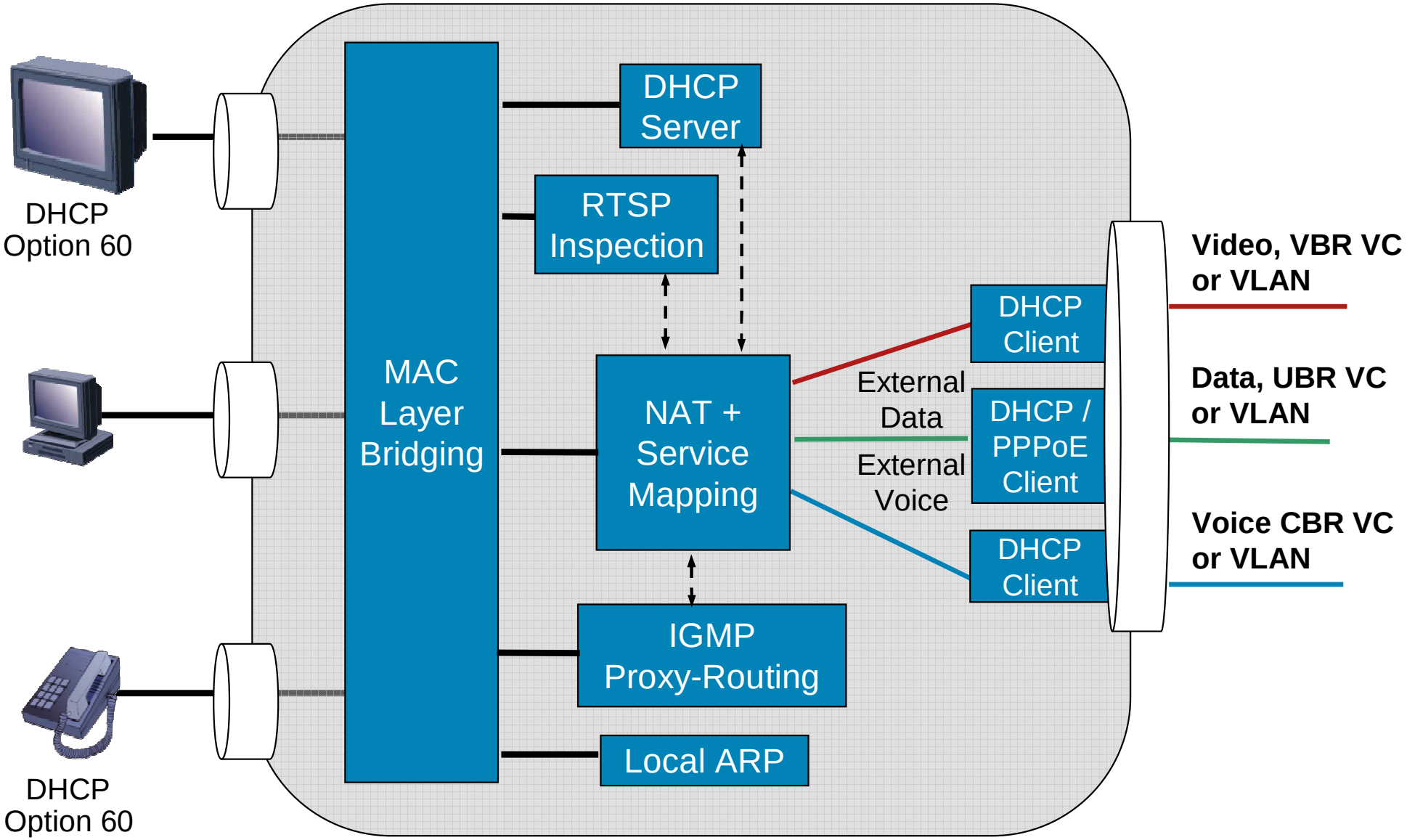
© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Home Access Gateway Architecture Layer 2



© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

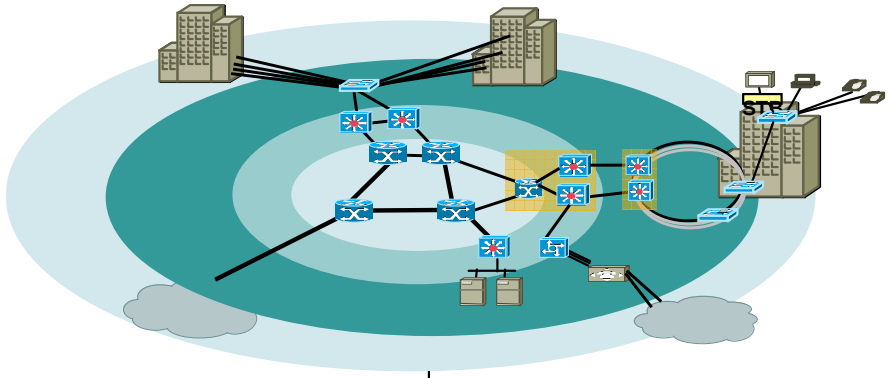
Home Access Gateway Architecture Layer 3 / NAT Capable - Multi VC



© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

In-House Connections
The Connected Home

FTTH Network



Residential Gateway

Gaming

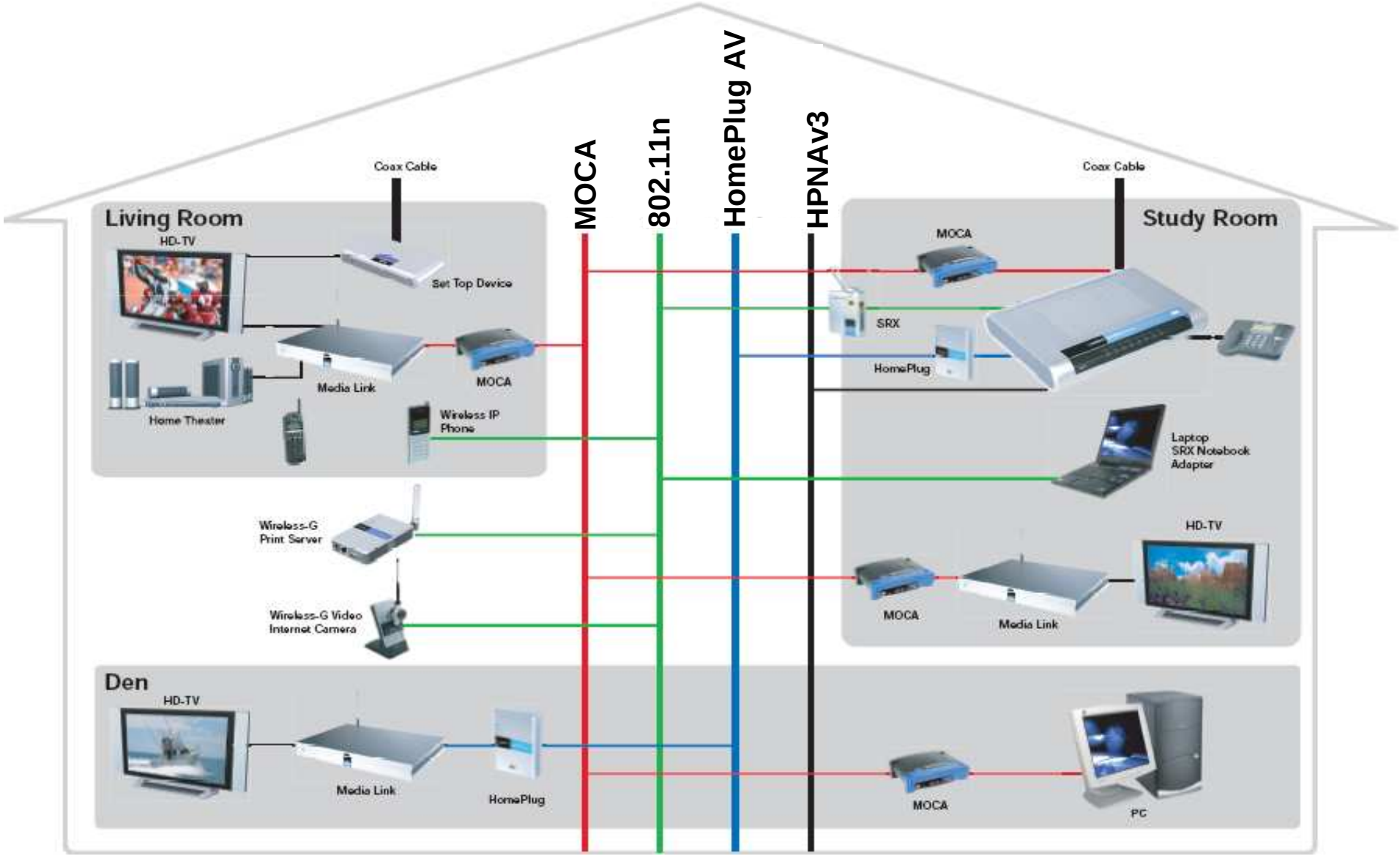
TV Service

Voice and Fax Service

Internet Service

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

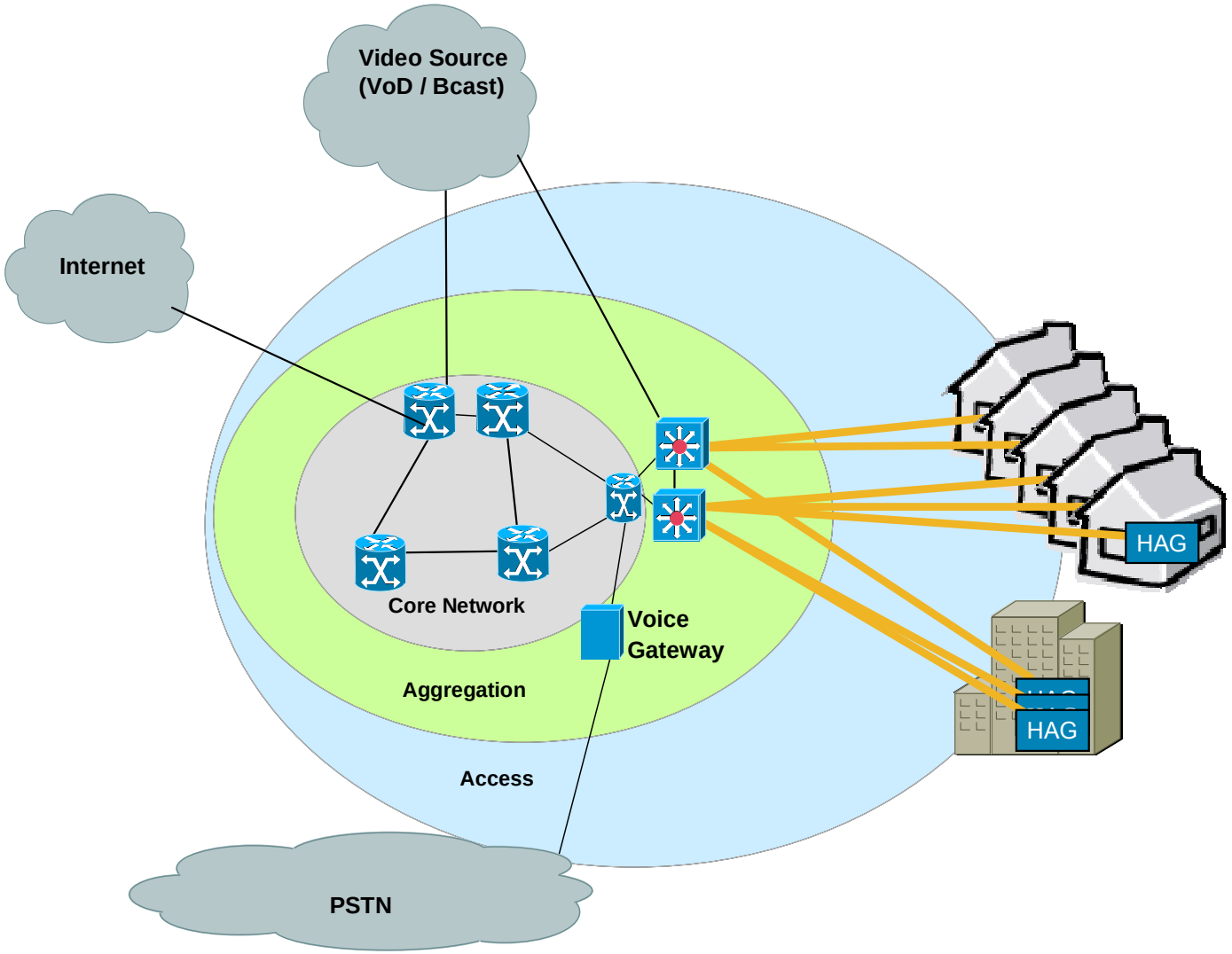
Multiple Networks in the Connected Home



NOTE: Newer dwellings may be wired Ethernet throughout

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

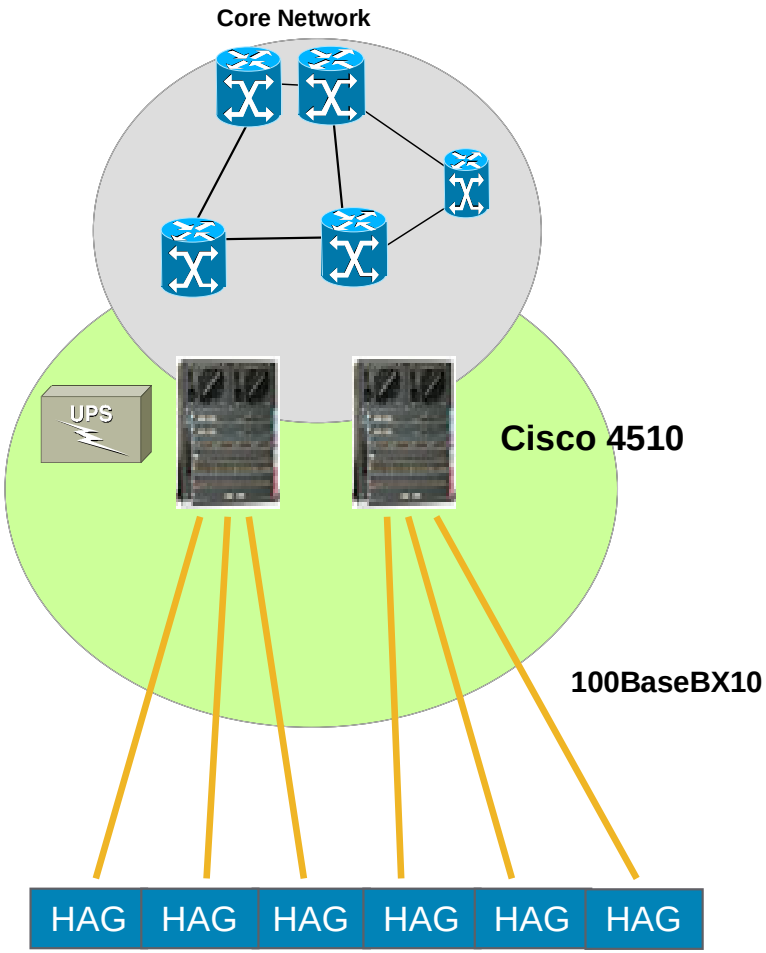
Centralized POP Approach



© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

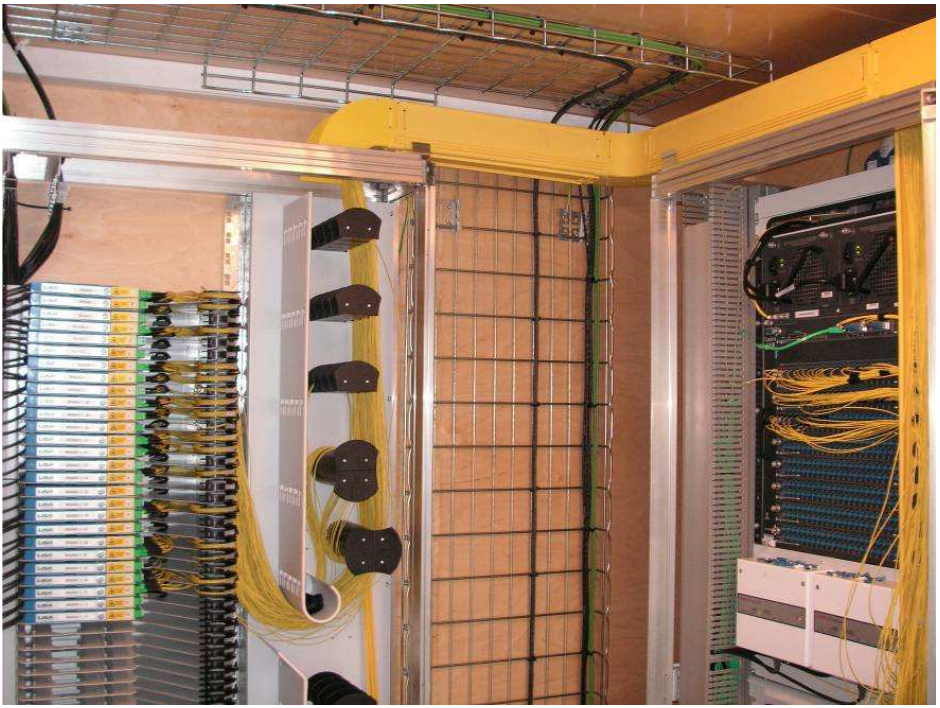
Centralized POP Approach

- 4510 with up to 384 ports
  - n x GE or 10GE uplinks
  - 3 x 4510 per 42RU Rack
  - 1182 Subscriber per Rack
- Pay as you grow
  - Modular line-card with SFP
  - Add (pay for) transceiver only when a subscriber is connected
- 100Mb/s per Subscriber
- Centralized Equipment
  - 1 point for AC and UPS
  - Central cable management and troubleshooting



© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Centralized Access Pop



ODF relative position to Cisco 4510R

Cisco 4510R in a rack

ODF

- Known POP sizes vary from 2 000 to 20 000 connected customers
- Citynet in Amsterdam has designed POP with 10 000 & 12 000 fibres
- New French Deployment (2M ports) with more than 30000 subscribers per Pop
- Loop lengths deployed: In average 3.5 km, maximum 5 km

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

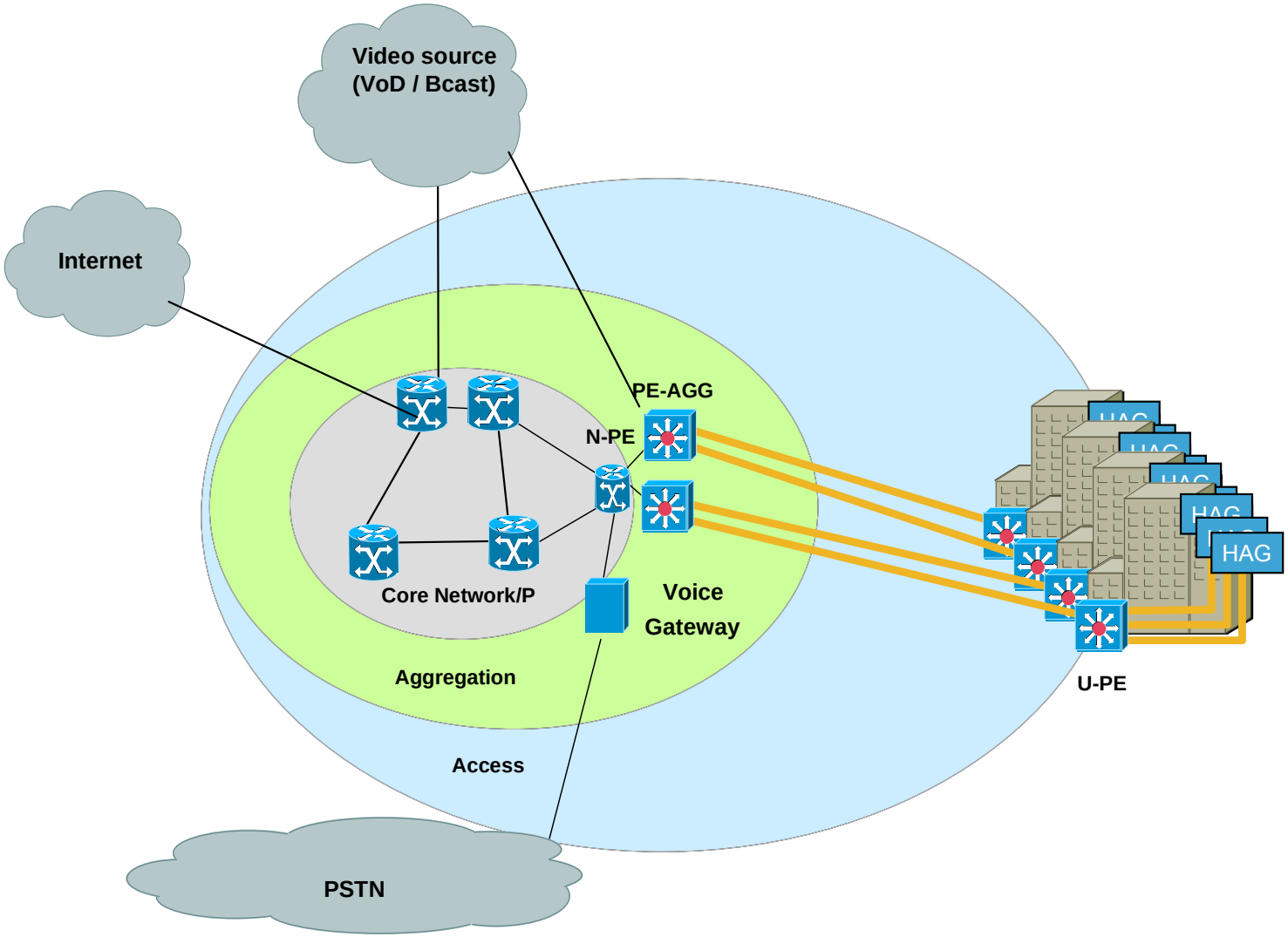
New Mechanical Solution

- ODF for 2304 fiber terminations
- Rack for 1152 active fiber interfaces
  - 50% take rate
  - up to 100% take rate achievable with second switch rack

Source: Huber & Suhner

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

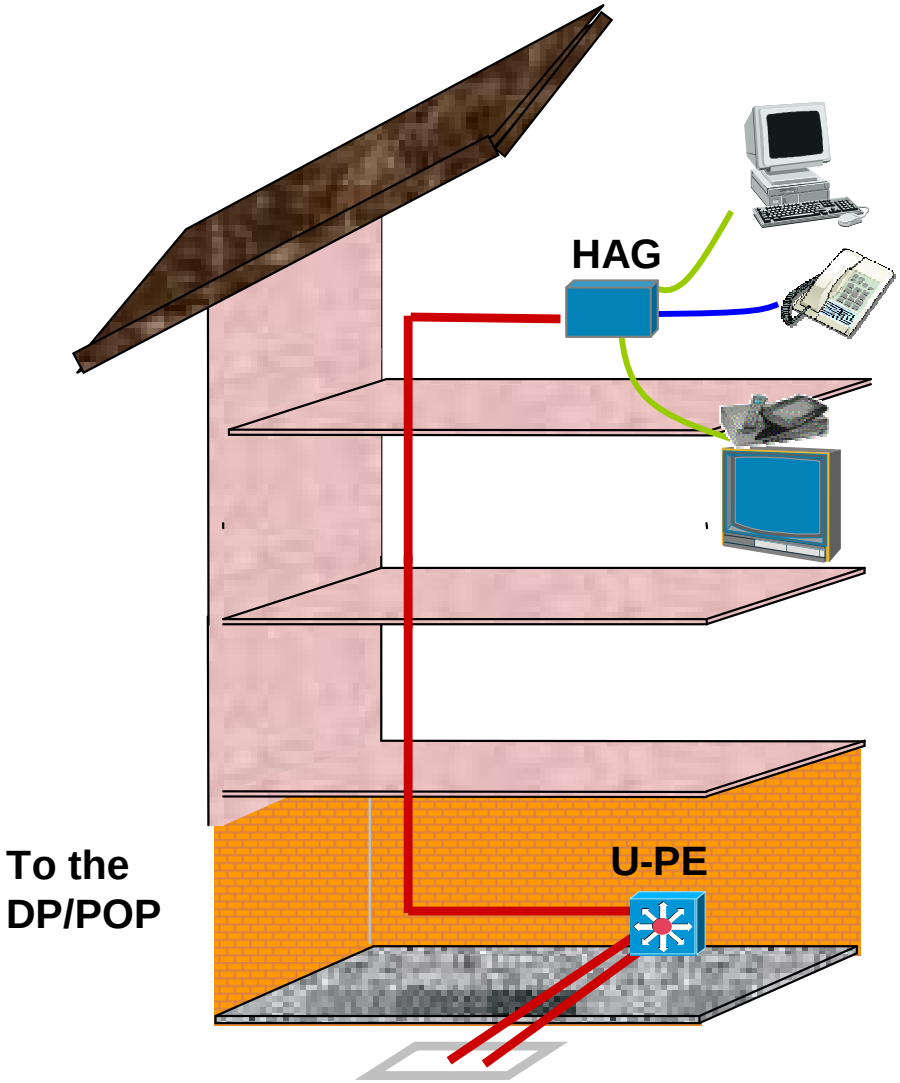
Distributed Access



© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Multi Tenant Building Solution Decentralized Access

Residential MTU Access



- Access Switch located in Basement/Utility Area
- UTP in-house cabling up to 90m distance

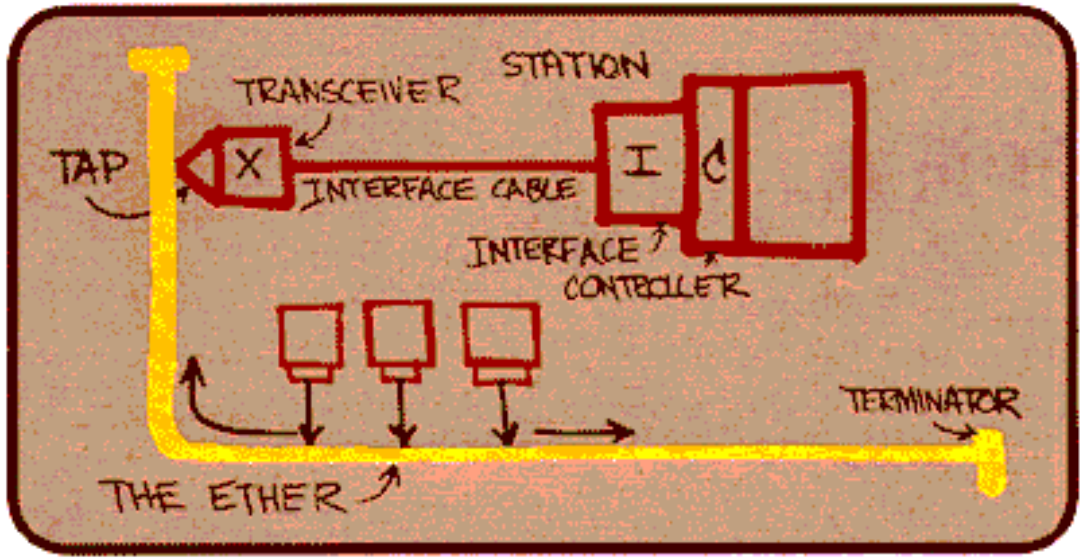
  Cost effective Deployment
- U-PE operates in L2 Mode and can provides access for Business services Layer2 & Layer3 VPN services as well as for Layer3 3Play services
- GE (L2) link(s) to the PE-AGG

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

FTTH Architecture Overview

© 2009 Cisco Systems, Inc. All rights reserved.

SP Ethernet Access



Metcalfe's Original Concept of Ethernet (1976)

- **Ethernet began as shared media tap points for workstations & bridges**
- **Leverage the multipoint nature of Ethernet in SP access. There is a *lot* of value here…**

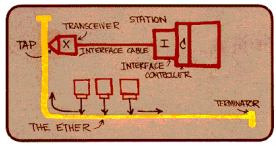
  Service Insertion Point Economics

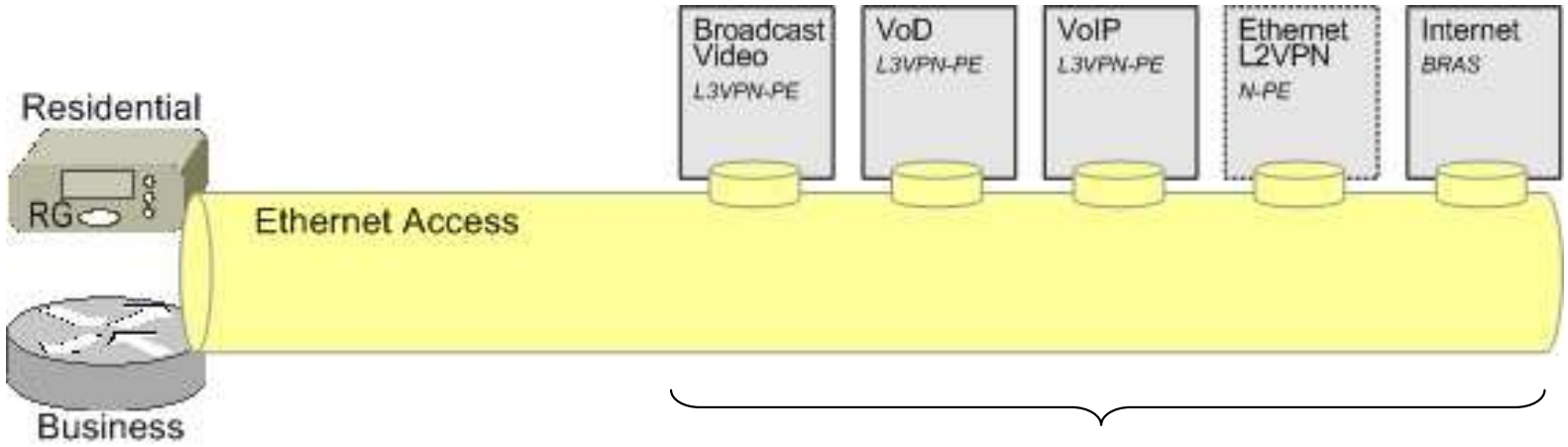
  Multipoint Services (Multicast)

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Multi-Edge Architecture

View from CE: Ethernet Tap Points by Application



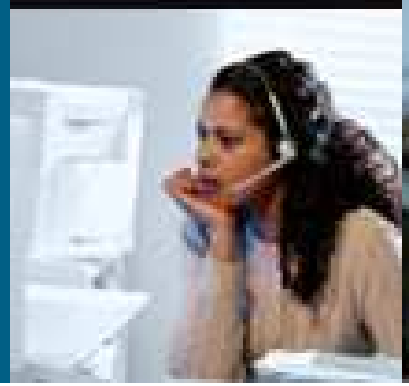


Modular L3 Edge → Ethernet Tap Points

- **Different L3 Edge by service, services can be added and managed independently**
- **SP Edge physically could be one L3 box, but likely is many**
  - Supports Geographic segmentation of application servers
  - Allows the use of distributing IP on a per service basis (e.g. multicast!), rather than using L2
  - Services needing per subscriber policies (internet, peer2peer, Lawful Intercept) inserted centrally, while ‘simpler’ services (IPTV, VoD) are distributed
- **Allows services & transport to be reused across a variety of access technologies**
- **Intermediate tunneling technologies transparent to the CE .**

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Design Considerations



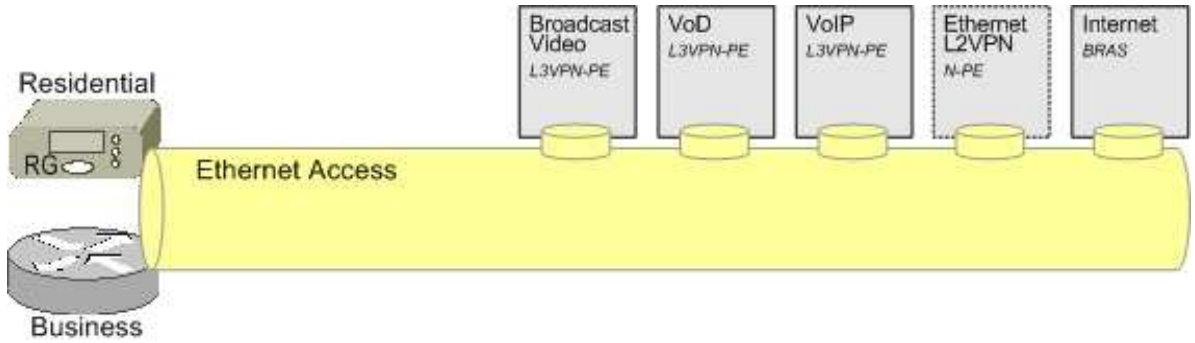
© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

E-FTTH Design Considerations

- Design Considerations
  - Service Delivery
  - Address Management
  - Subscriber Identification
  - User Isolation & Security
  - Network Resilience
  - QoS

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Design Considerations
Service Delivery



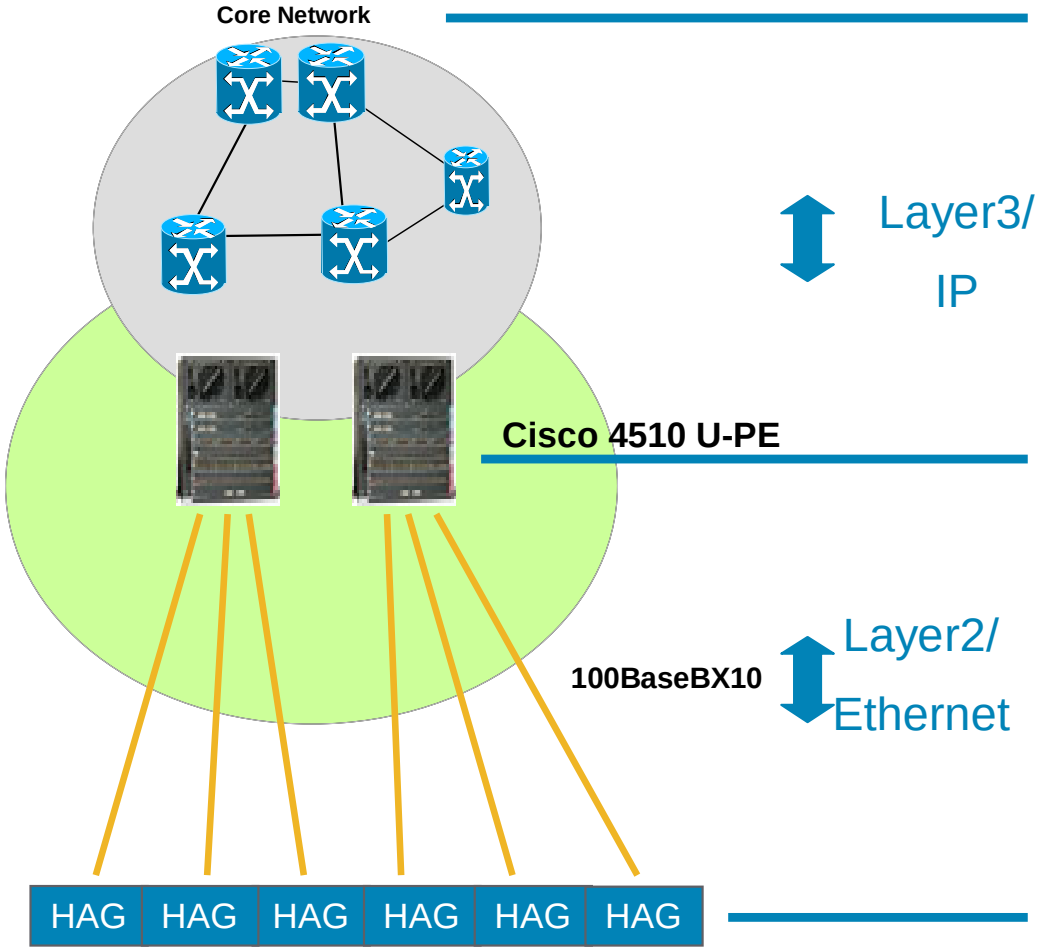
© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Service Delivery

- Several Approaches are chosen for service delivery
- FTTH providers and alternate SP choose pure IP delivery
  - L3 boundaries either on access device or aggregation device
- PTTs and SP with existing xDSL services choose a mixed approach
  - PPPoE for Data to leverage existing Subscriber infrastructure
  - DHCP/IP for Voice and Data to leverage native service delivery (VoIP, IP Multicast)
  - In Line with DSL Forum TR-101 and HGI

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

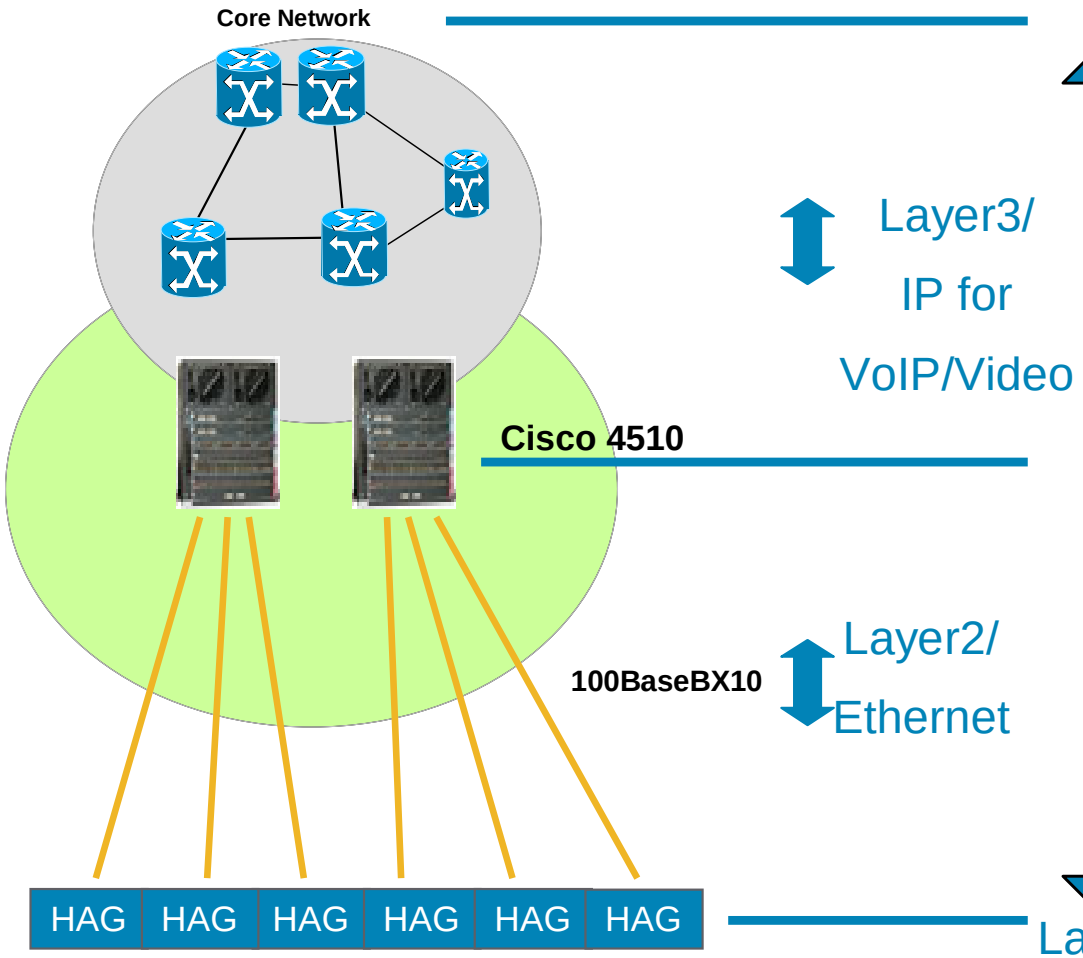
Service Delivery
Centralized Access – All IP



- U-PE with up to 384 Subscribers
  - IP/L3 termination on U-PE
- Prevents L2 Scaling Issues
  - MAC, BCAST
- Native L3 support for IP based services
  - Decentralized Service Insertion
- L3 Multicast delivery up to the U-PE

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Service Delivery
Centralized Access – IP and PPPoE



Layer3/
IP for
VoIP/Video

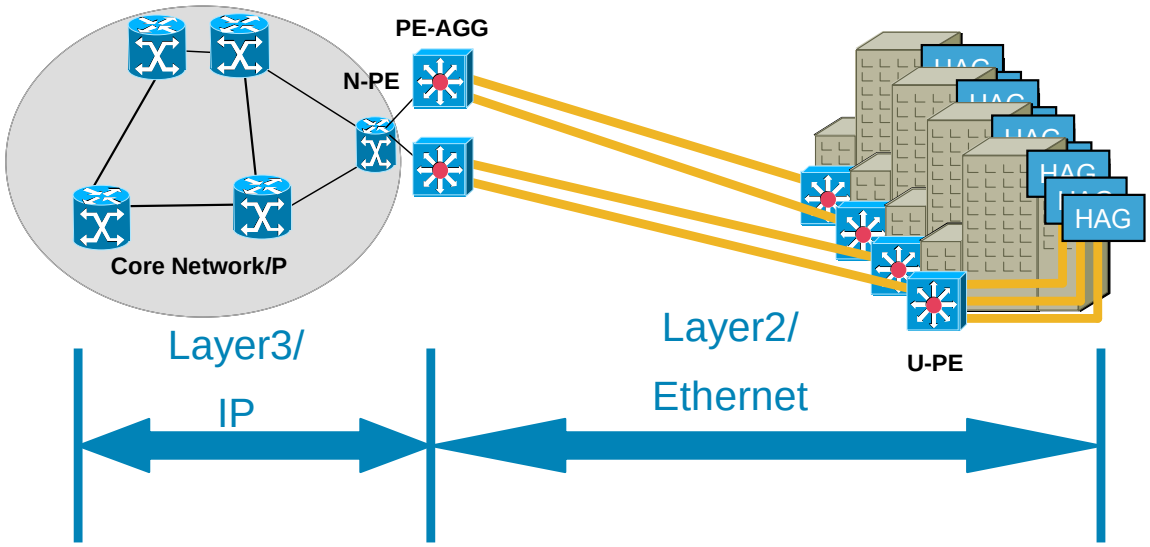
Layer2/
Ethernet

Layer2/
PPPoE
For Data

- U-PE with up to 384 Subscribers
  - Hybrid L2/L3
- L2 transport for PPPoE
  - Requires MAC, VLAN scaling
- Native L3 support for IP based services
  - Decentralized Service Insertion for Voice and Video
- L3 Multicast delivery up to the U-PE

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

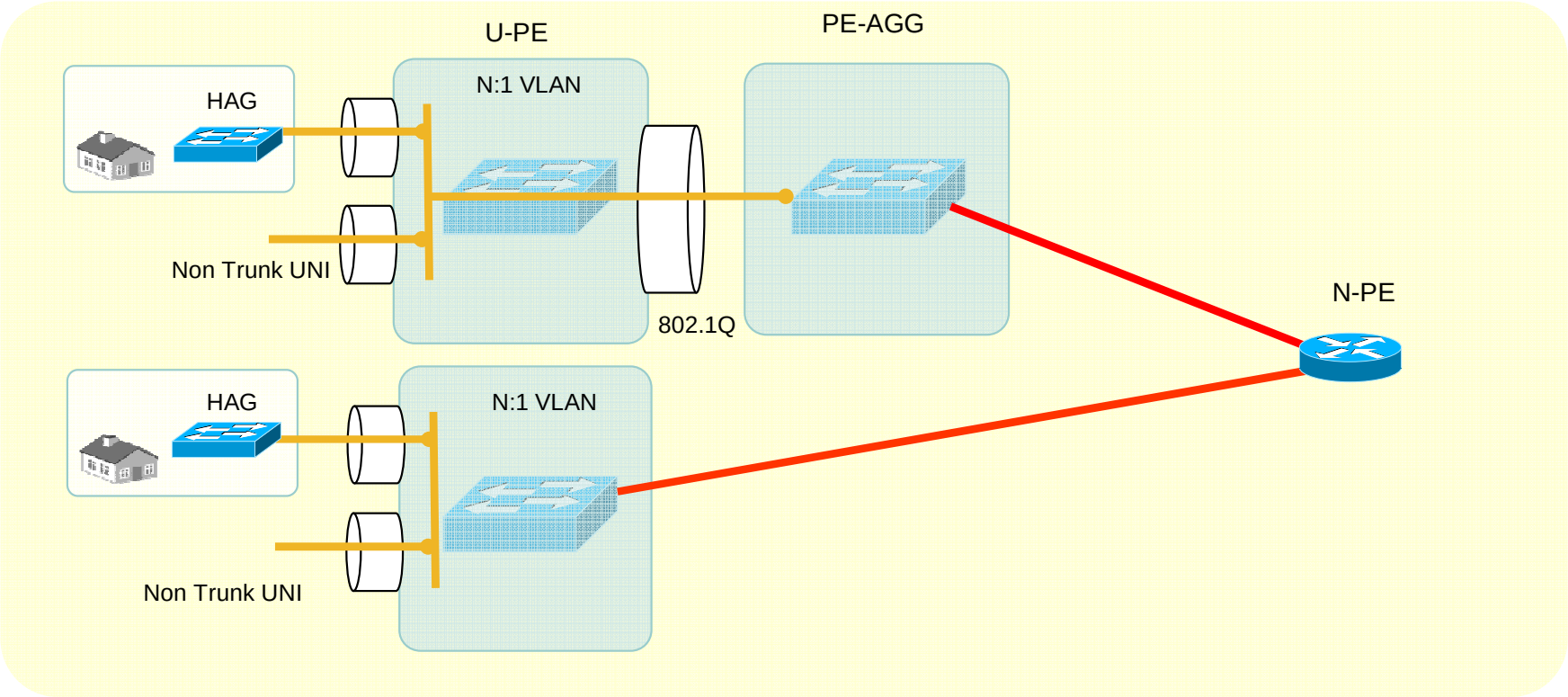
Service Delivery
Distributed Access



- U-PE with up to 24 subscribers in L2 Mode
  - –IGMP Snooping for IP/MC
- PE-AGG in L3 Mode
  - –Alternative Hybrid L2/L3 for PPPoE
- IP Multicast delivery to PE-AGG
  - –IGMP Snooping on U-PE

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Services Connectivity
Non Trunk UNI, N:1 VLAN

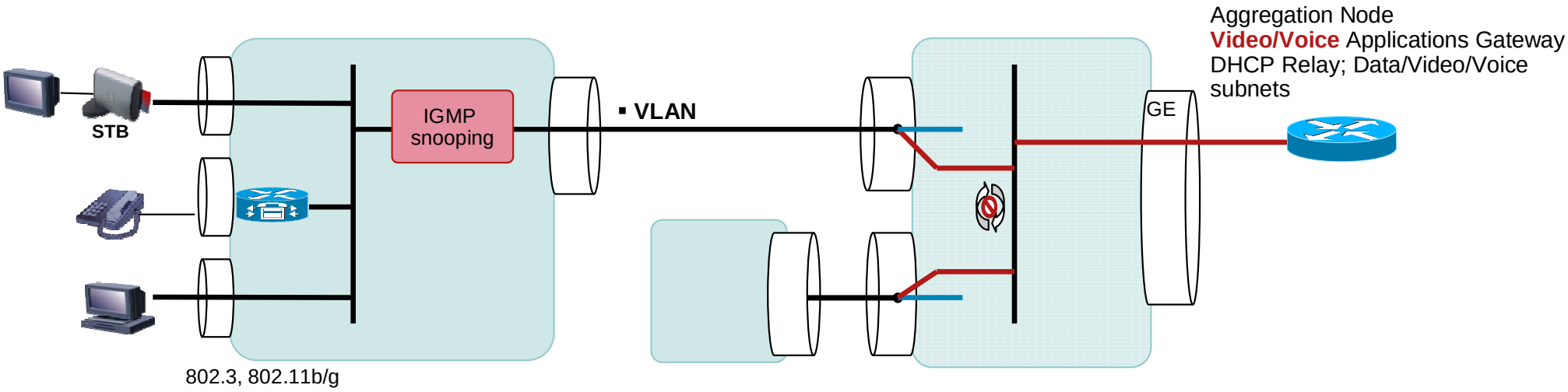


- Single VLAN per U-PE or group of U-PE's
  - 😐 IP address ranges per service (secondary addresses)
  - ☺ HAG does not need to support 802.1Q trunking
- Ease of use:
  - ☺ all HAG data ports are equal (no mis-wiring)

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Access Node Service Mapping (Bridged HAG)

Non-Trunk UNI, N:1 VLAN Connectivity



- **Service Connectivity and Forwarding**
  - Single VLAN
  - Limited MAC switching
  - IGMP Snooping
- **Service Prioritization**
  - Ethernet Cos based

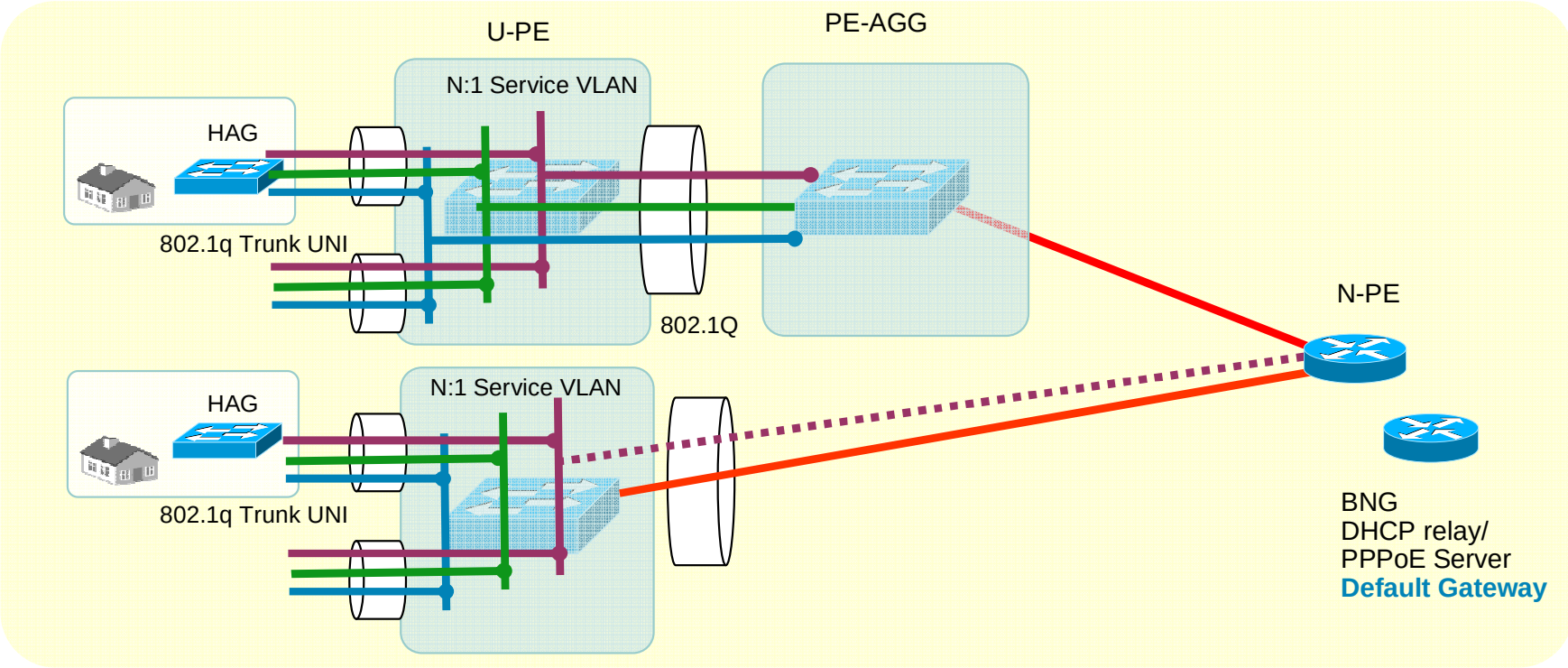
- **Service Connectivity and Forwarding**

Data/Voice/Video - IPoE: bridge into N:1 data/voice/video service VLAN

- **Service Prioritization on UNI**
  - Ethernet CoS based
- **Service Prioritization on NNI**
  - Ethernet CoS based

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Services Connectivity
Trunk UNI, N:1 Service VLAN

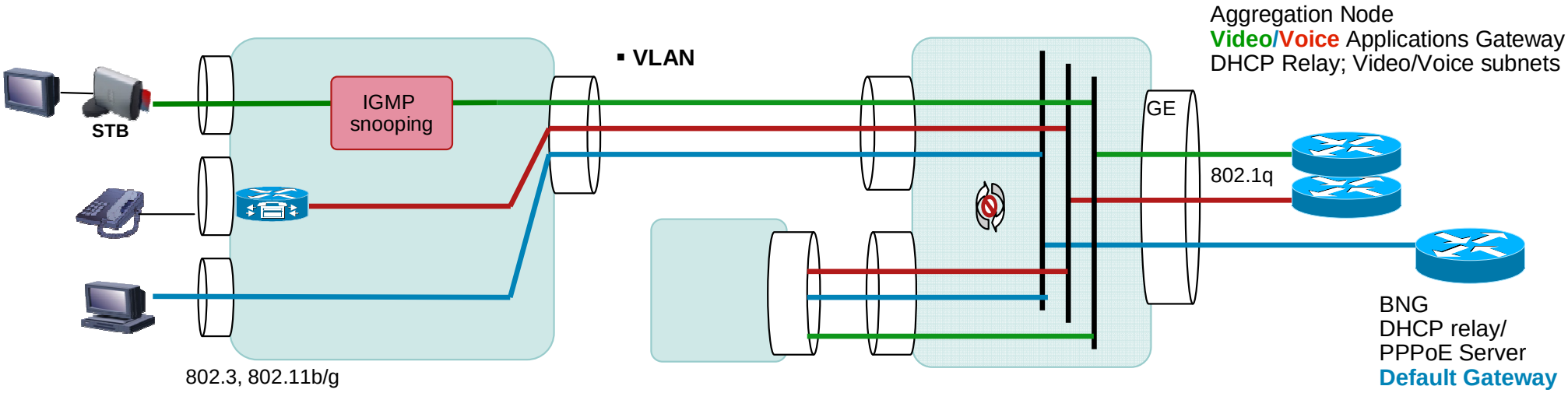


- VLAN per Service
  - ☺ IP address ranges per service (can overlap)
  - ☹ HAG has to support 802.1Q trunking, and needs provisioning
  - 😐 Supports L2/L3 Hybrid (e.g. L3 for Voice&Video, L2 for PPPOE)
- Ease of use:
  - ☹ HAG data ports are now service specific (potential mis-wiring)

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Access Node Service Mapping (Bridged HAG)

Trunk UNI, N:1 VLAN Connectivity



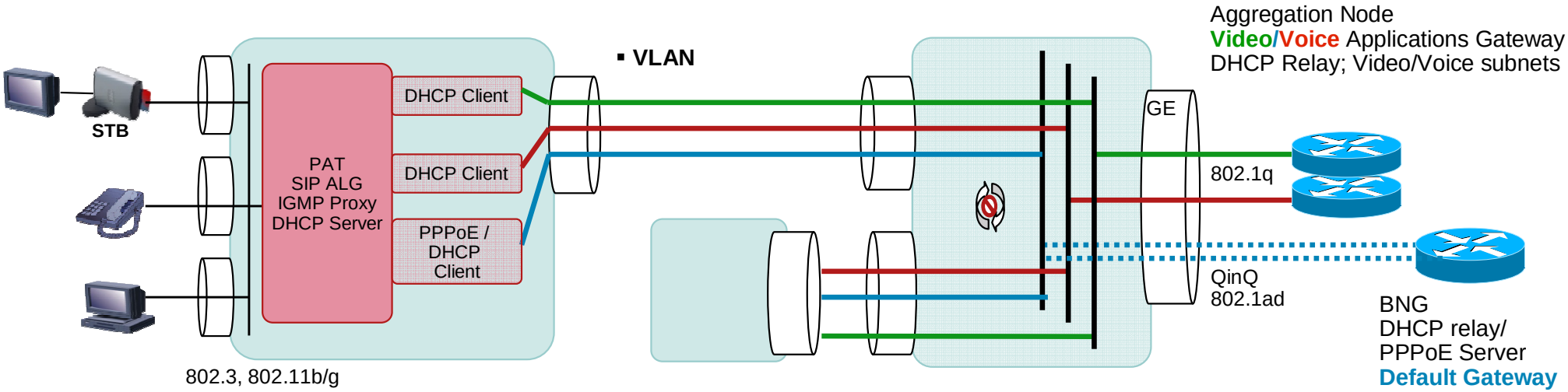
- **Service Connectivity and Forwarding**
  - Single VLAN per services
  - Limited MAC switching)
  - IGMP Snooping (multi-STBs)
- **Service Prioritization**
  - Ethernet Cos based

- **Service Connectivity and Forwarding**
  - IA: Bridge into N:1 VLAN IA service VLAN
  - Voice: bridge into N:1 voice service VLAN
  - Video: bridge into N:1 video service VLAN
- **Service Prioritization on UNI**
  - Ethernet CoS based
- **Service Prioritization on NNI**
  - Ethernet CoS based

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Access Node Service Mapping (Routed HAG)

Trunk UNI, 1:1 VLAN Connectivity for Internet Access

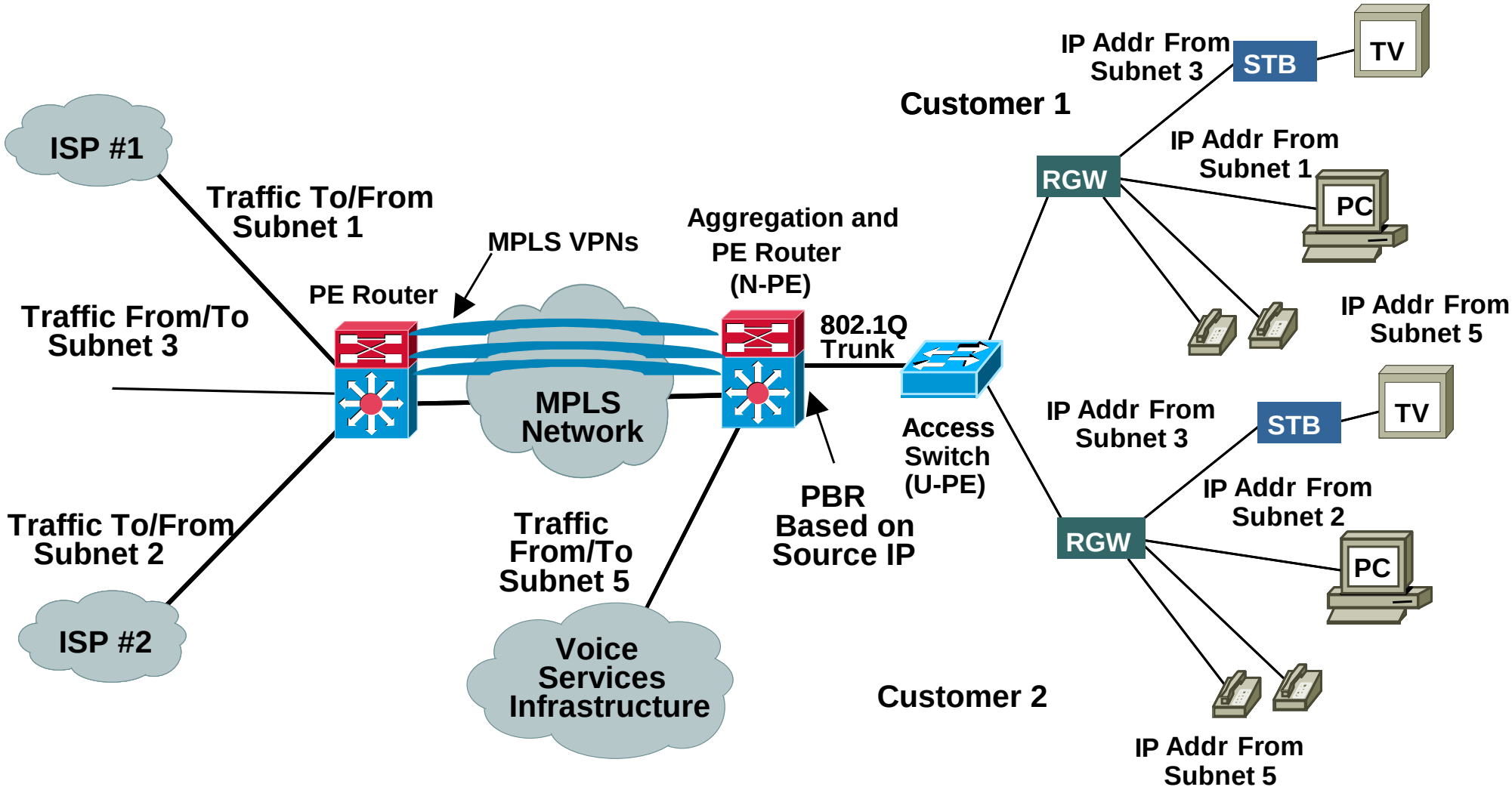


- **Service Connectivity and Forwarding**
  - Routing based on service destination or home device mapping
  - Configuration by GUI, DHCP Op. 121 or TR-069 OSS
- **Service Prioritization**
  - Ethernet Cos based
- **Other Services functions**
  - IGMP Proxy-routing, SIP NAT ALG, PAT, RTSP NAT ALG

- **Service Connectivity and Forwarding**
  - IA: 1:1 VLAN IA service VLAN
  - Voice: bridge into N:1 voice service VLAN
  - Video: bridge into N:1 video service VLAN
- **Service Prioritization on UNI**
  - Ethernet CoS based
- **Service Prioritization on NNI**
  - Ethernet CoS based

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Open Access:
Single VLAN With PBR Architecture



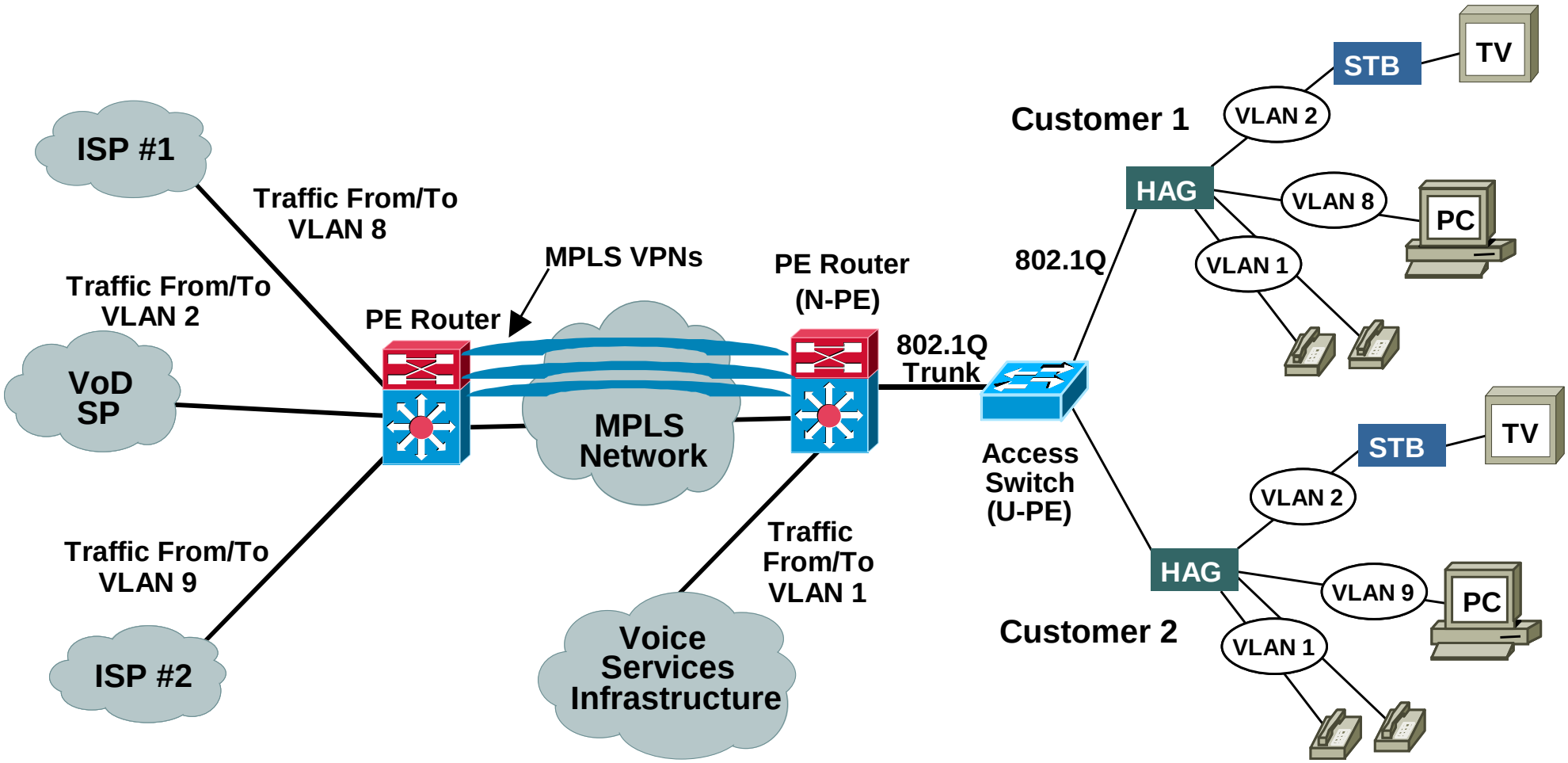
© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Single VLAN with Policy Based Routing (PBR)

- One VLAN per switch (U-PE) or per ring (based on PVLAN Support)
- No specific requirements for CPEs (no VLAN functionality)
- Multiple per-SSP address scopes by secondary addresses on N-PE (for downstream traffic)
- Upstream PBR based on source address into SSP specific VLAN
- VLAN to MPLS VPN/VRF mapping with „Source IP Address VRF Select“ feature
- DHCP server identifies subscriber via Option 82 and the appliance via MAC address or DHCP option 60 to allocate from proper address pool
- DHCP Snooping/IP Source Guard ensures that only valid packets are accepted from customer, prevents IP spoofing and using unassigned IP addresses

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Open Access: Per-SP VLAN Architecture



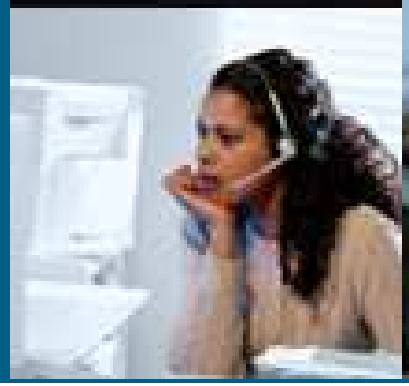
© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Per SP VLAN

- Every customer sees a VLAN per SP at his UNI
- CPE must be VLAN-enabled (e.g. switch)
- Use PVLANs on Rings to scale VLAN id‘s
- Use hub and spoke with PVLAN trunk on Cat 4k as AGG-PE
- DHCP server identifies subscriber via Option 82 and the appliance via MAC address or DHCP option 60 to allocate from proper address pool
- VLAN interfaces map directly into MPLS VRF/VPN

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Design Considerations
Address Management



© 2009 Cisco Systems, Inc. All rights reserved.

IP Address Management

- Mix of public and private IP addresses
  - Public addresses for Internet Access
  - Private addresses for services “not leaving” the network:
    - VoIP
    - Broadcast Video
    - Video-on-Demand

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

IP Address Management

- DHCP is widely used to provide IP addresses to Network Elements and Subscribers
- DHCP Server issues proper IP address based on:
  - Location of Subscriber (DHCP Option 82)
  - Vendor ID of CPE originating request (DHCP Option 60 and/or Vendor ID i.e. the first three bytes of MAC-Address)
- This enables per service IP Address assignment
- Simplified Security and QoS Classification through Service Address Ranges
- Voice, Video and Data can all reside on the same Access VLAN
  - Removes the need for 802.1Q trunking on the Home Access Gateway
  - More Secure and simpler Home Access Gateway implementation
  - Uses Secondary IP Addresses on the L3 Distribution Switches
    - *VLAN Per Service is supported if needed/desired*

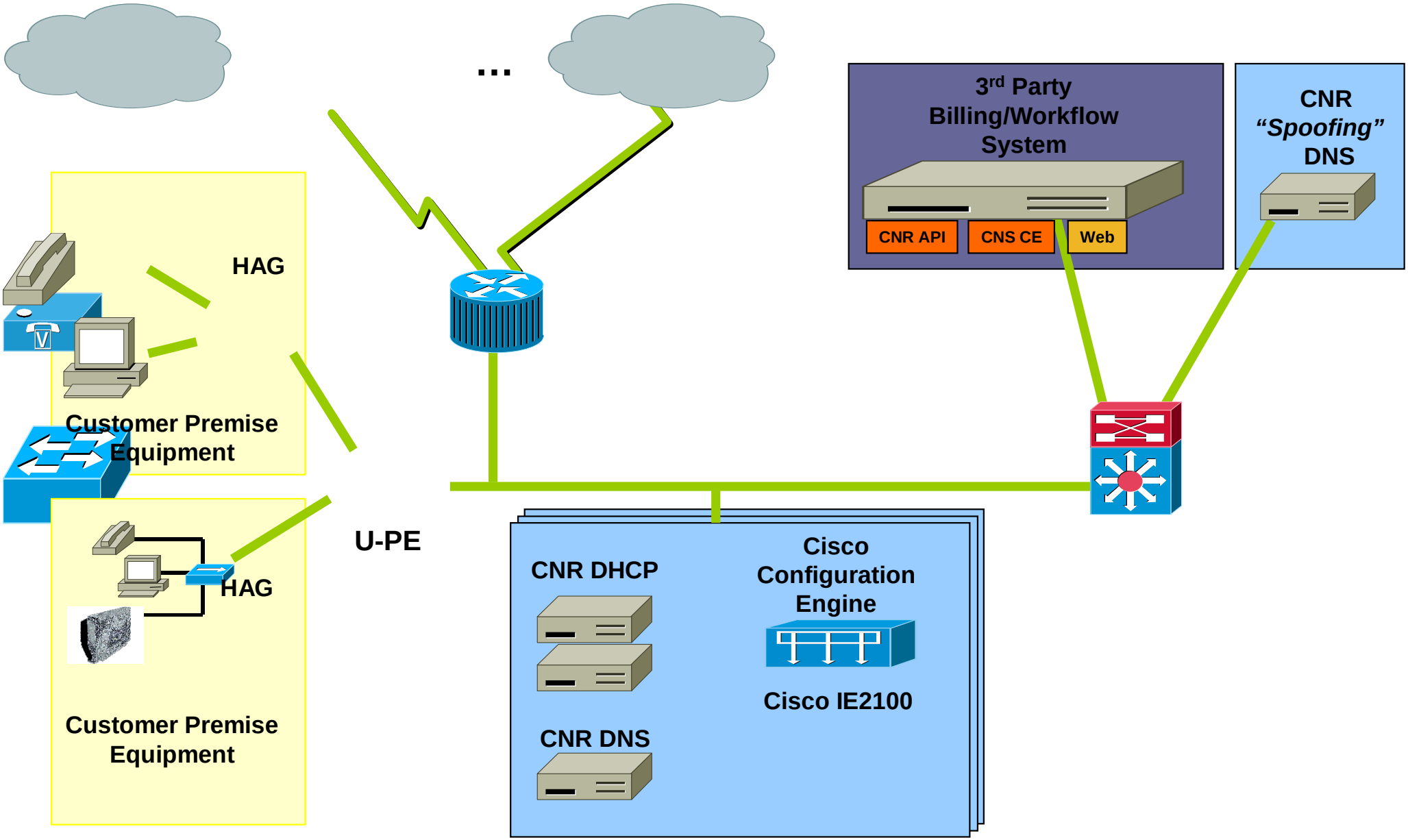
© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Subscriber Provisioning

- Cisco Partner Applications
- Support both self and CSR-assist provisioning
- Allows subscriber to request new services and make changes to existing services
- Handles device configuration behind the scene
- Supports Web-based interface for subscribers to register for services
- Provides login portal for new subscribers
- Implements option 82

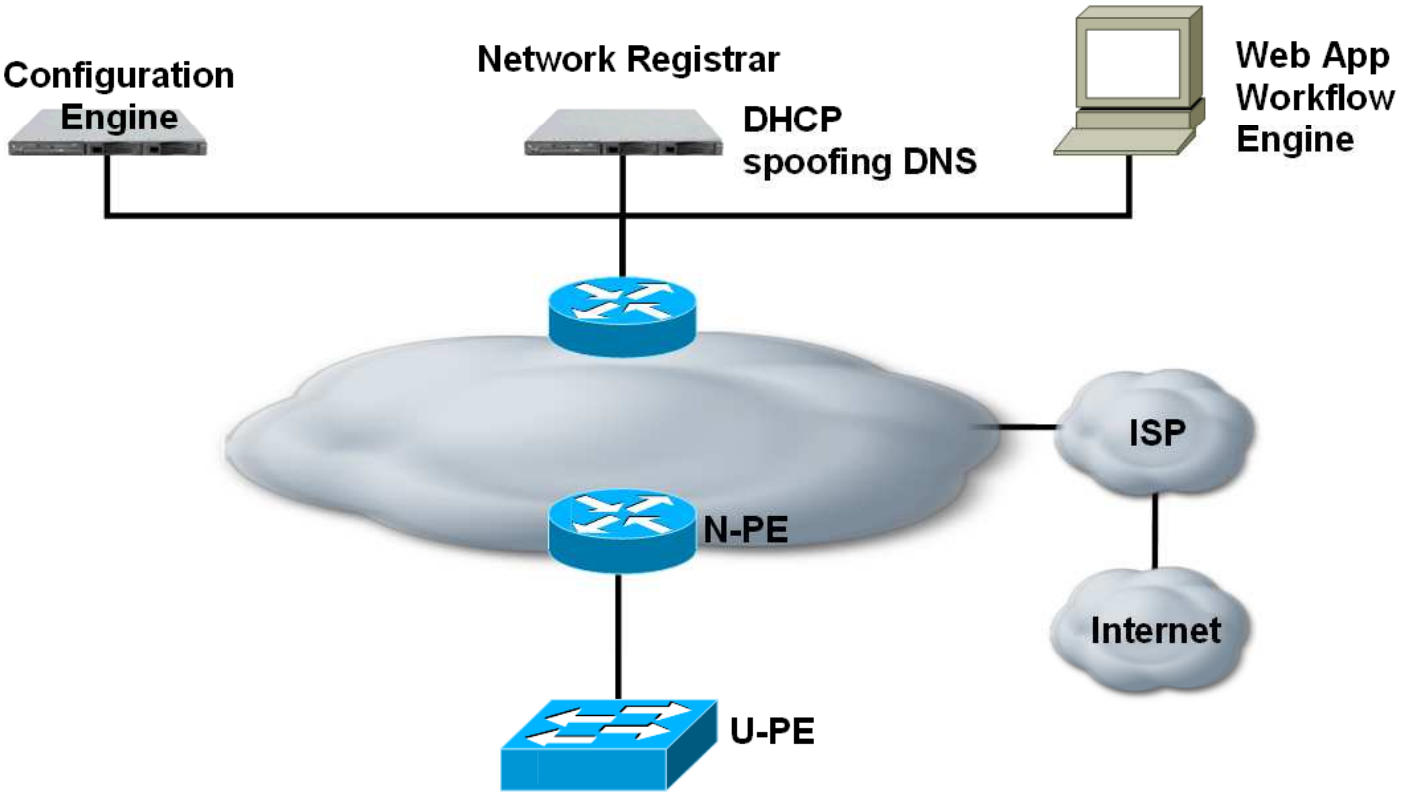
© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Generic Provisioning Platform



© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

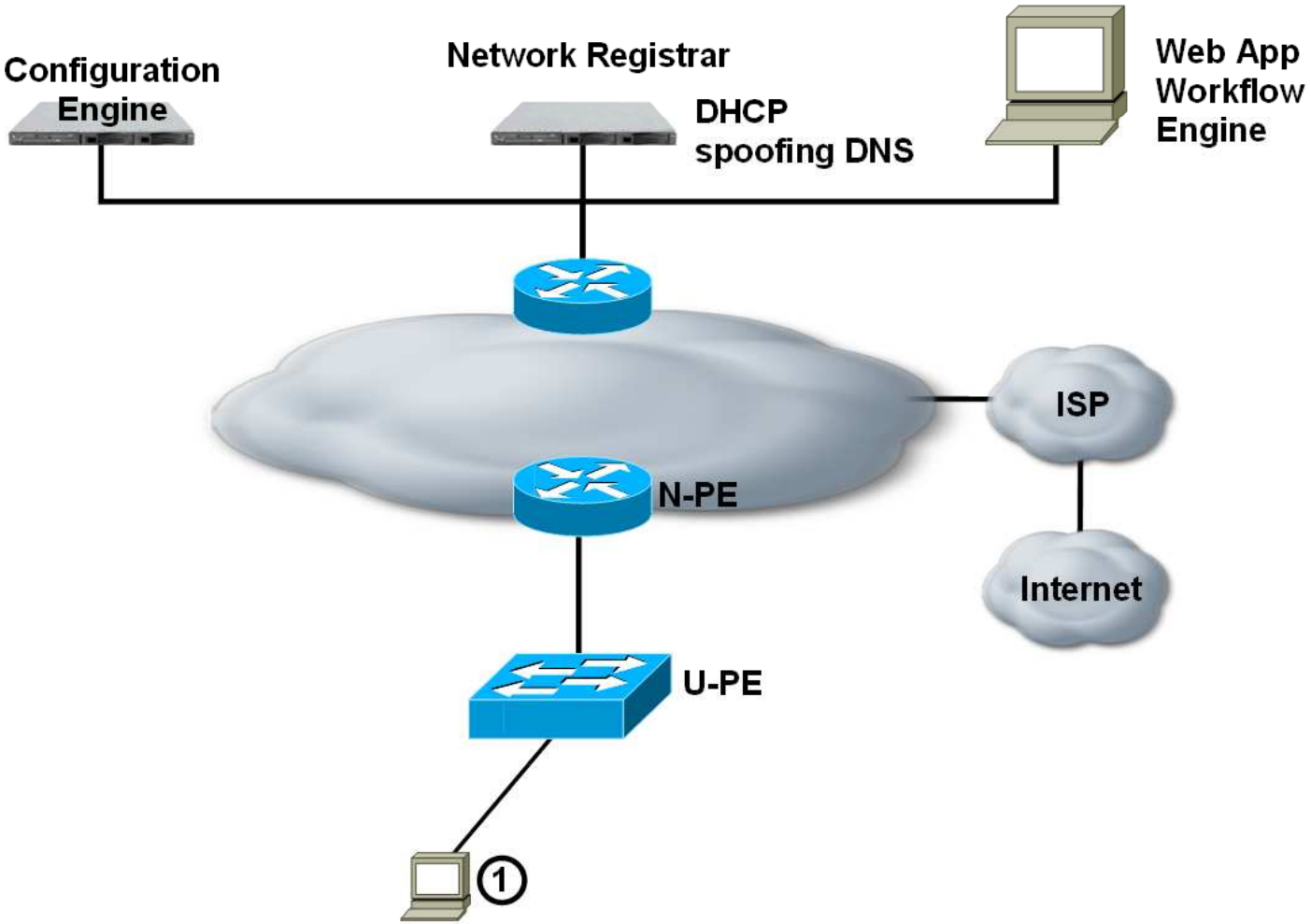
Self-Provisioning Workflow



© 2009 Cisco Systems, Inc. All rights reserved.

Self-Provisioning Workflow

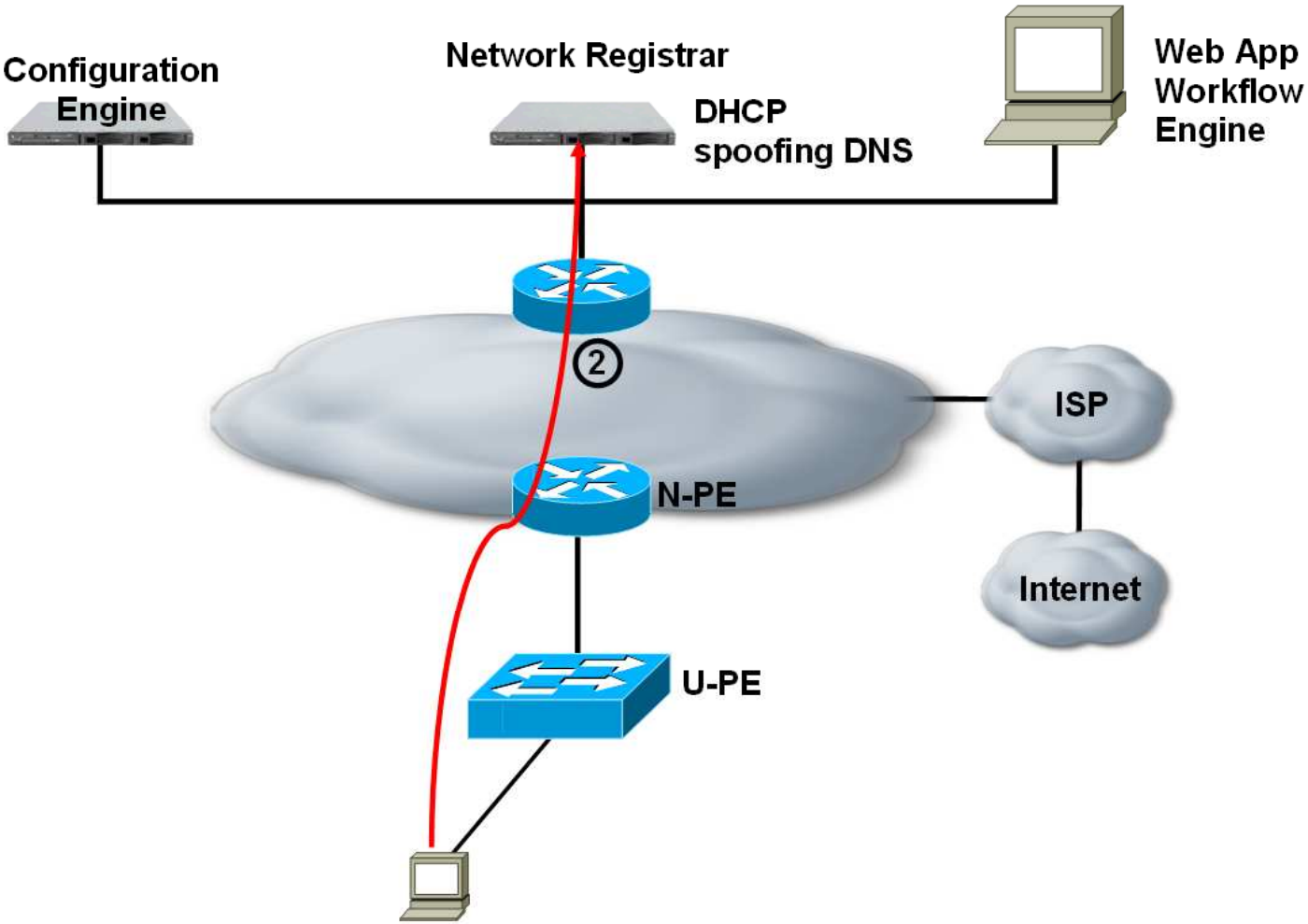
1. User plugs in PC



© 2009 Cisco Systems, Inc. All rights reserved.
Cisco Public

Self-Provisioning Workflow

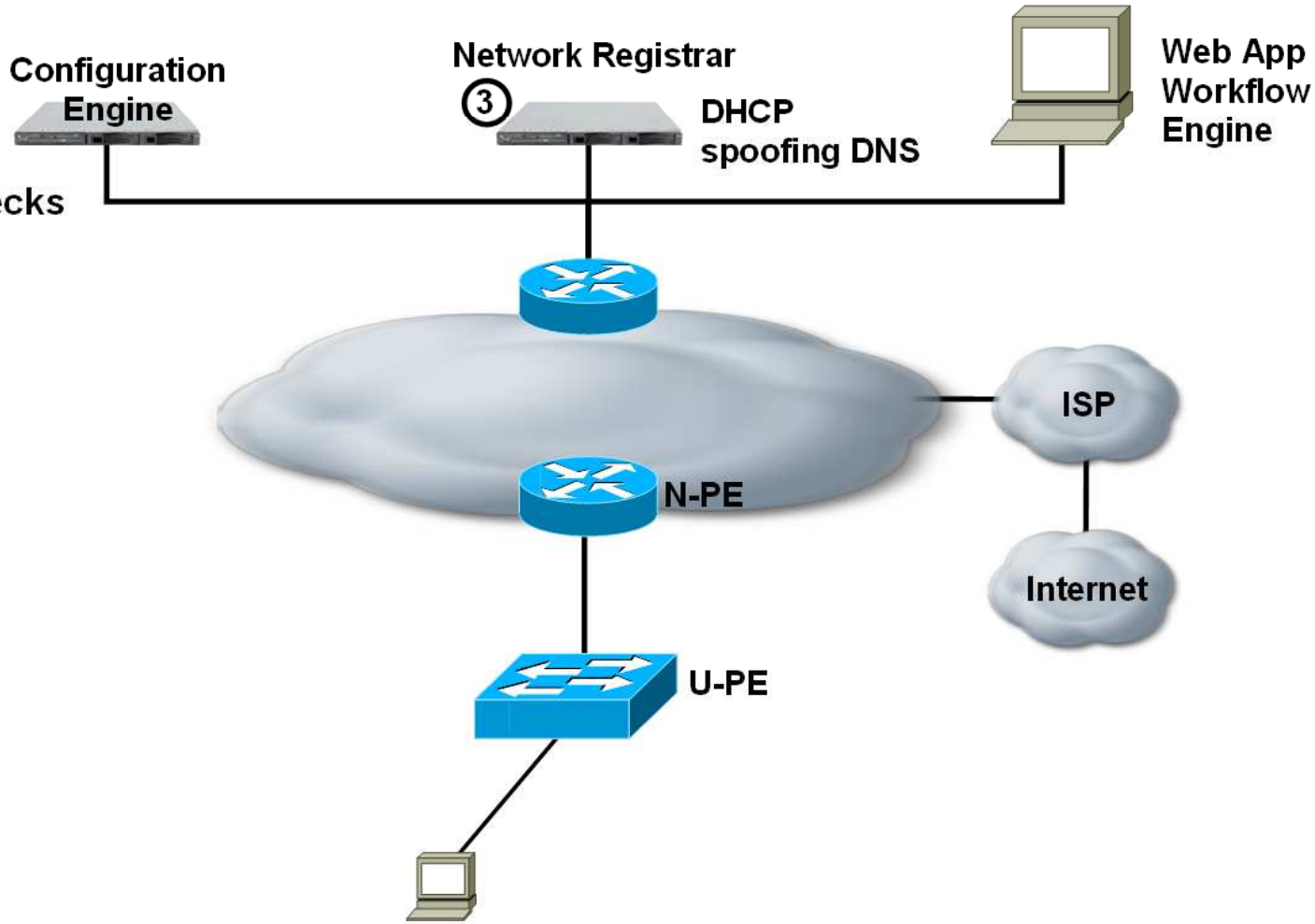
1. User plugs in PC
2. PC sends DHCP request; switch adds option 82



© 2009 Cisco Systems, Inc. All rights reserved.
Cisco Public

Self-Provisioning Workflow

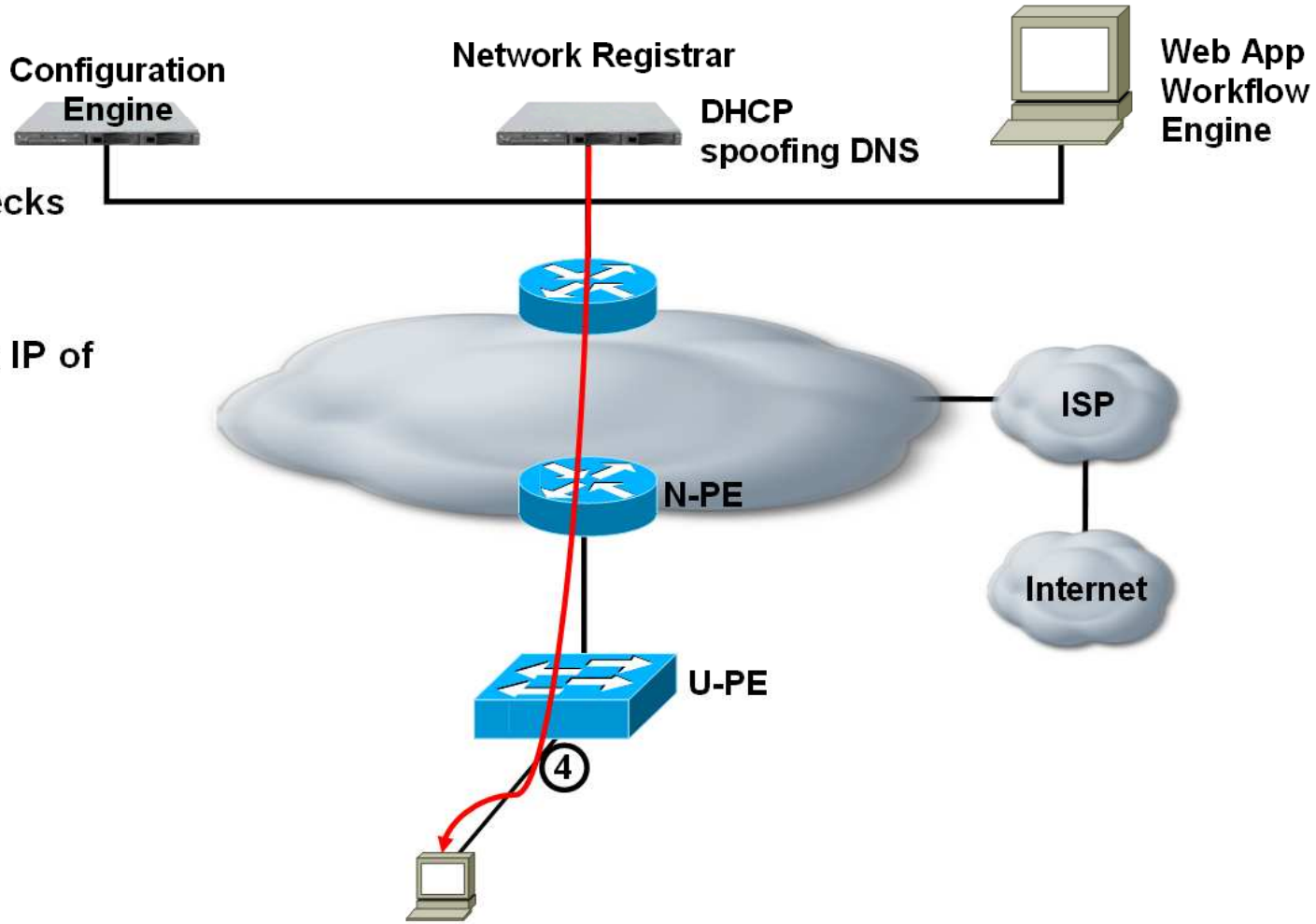
1. User plugs in PC
2. PC sends DHCP request; switch adds option 82
3. Cisco Network Registrar extracts option 82 and checks if client exists



© 2009 Cisco Systems, Inc. All rights reserved.
Cisco Public

Self-Provisioning Workflow

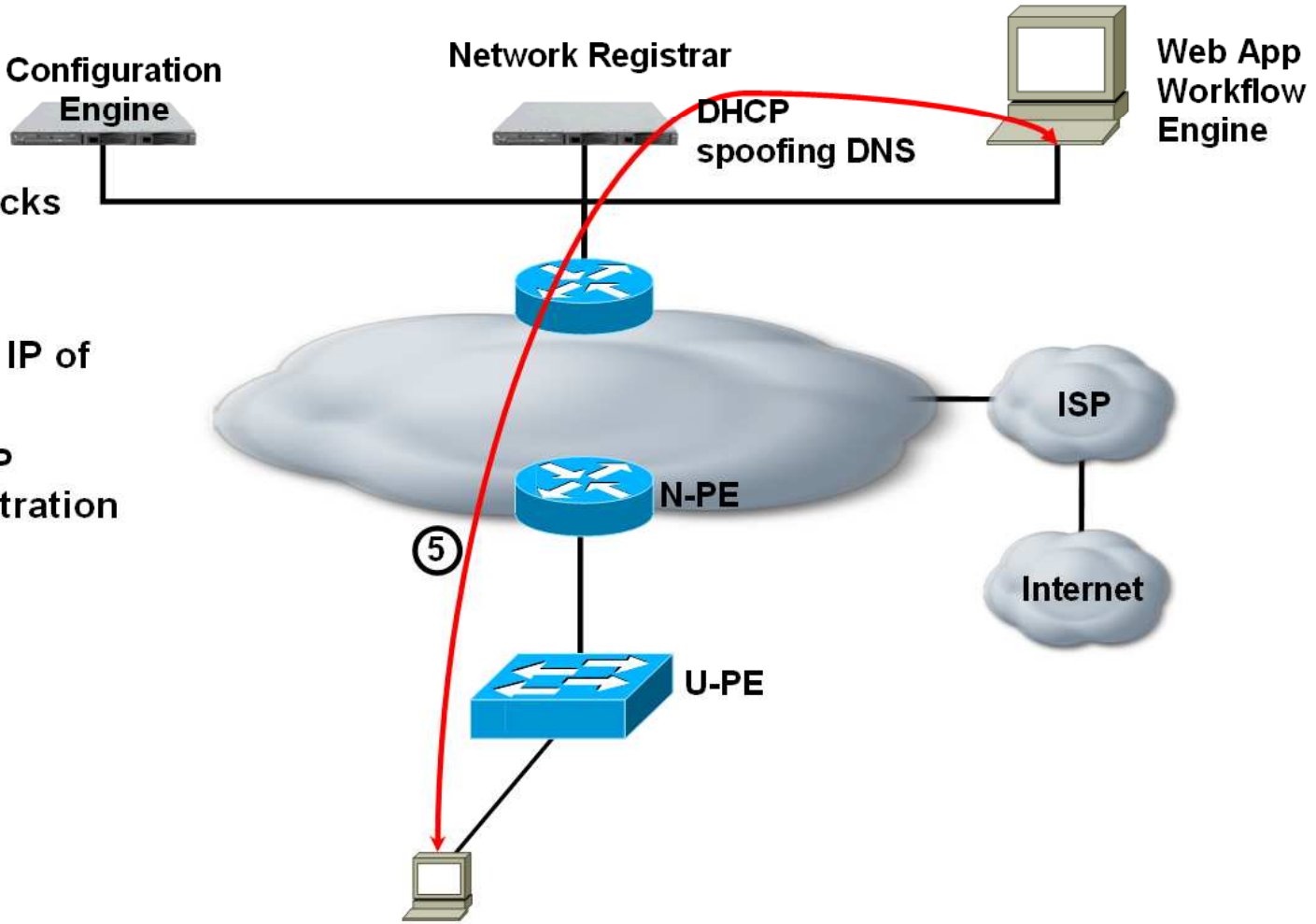
1. User plugs in PC
2. PC sends DHCP request; switch adds option 82
3. Cisco Network Registrar extracts option 82 and checks if client exists
4. No such client, so returns temporary IP address with IP of spoofing DNS server



© 2009 Cisco Systems, Inc. All rights reserved.

Self-Provisioning Workflow

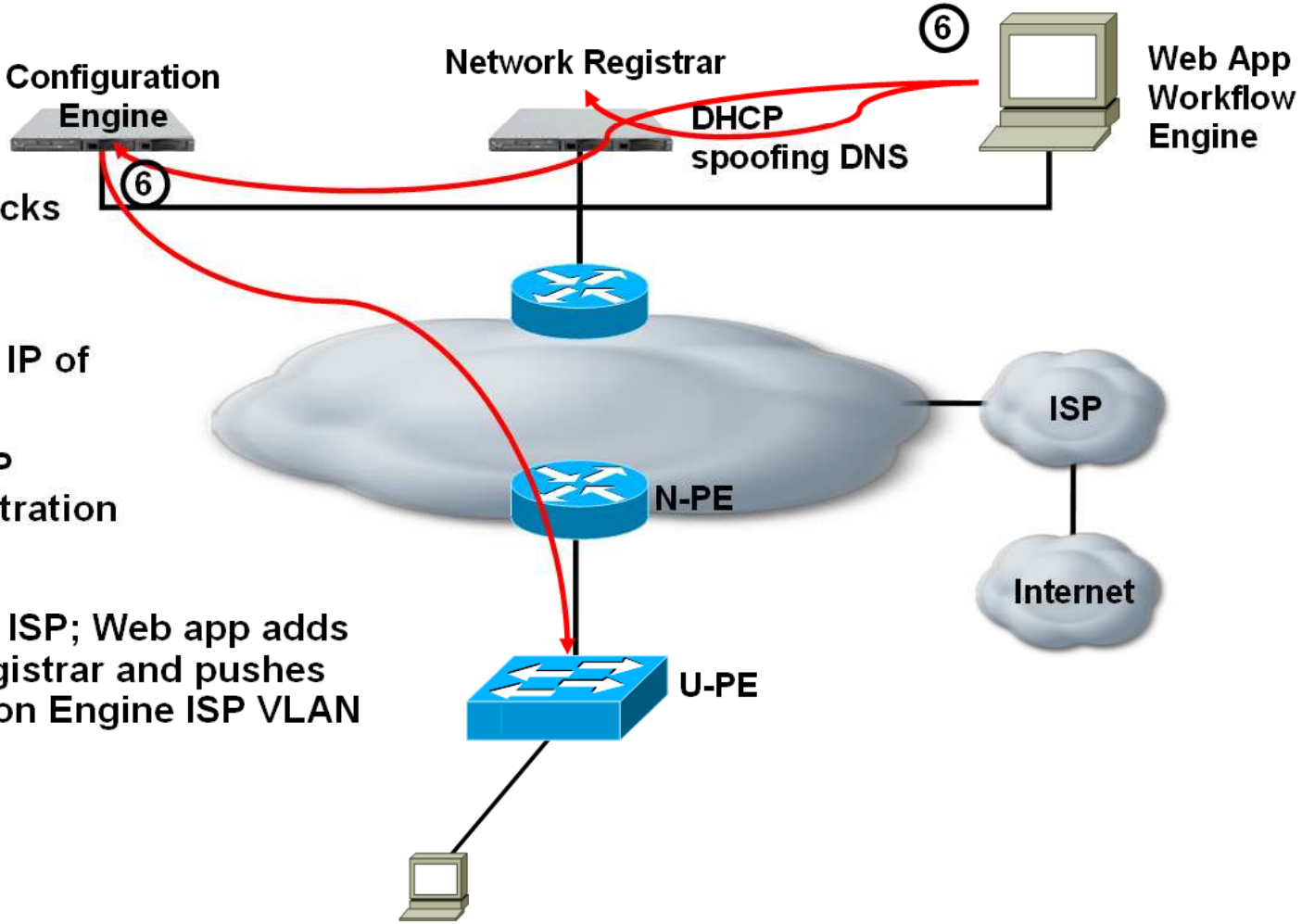
1. User plugs in PC
2. PC sends DHCP request; switch adds option 82
3. Cisco Network Registrar extracts option 82 and checks if client exists
4. No such client, so returns temporary IP address with IP of spoofing DNS server
5. User opens browser; HTTP request redirected to registration app by spoofing server



© 2009 Cisco Systems, Inc. All rights reserved.
Cisco Public

Self-Provisioning Workflow

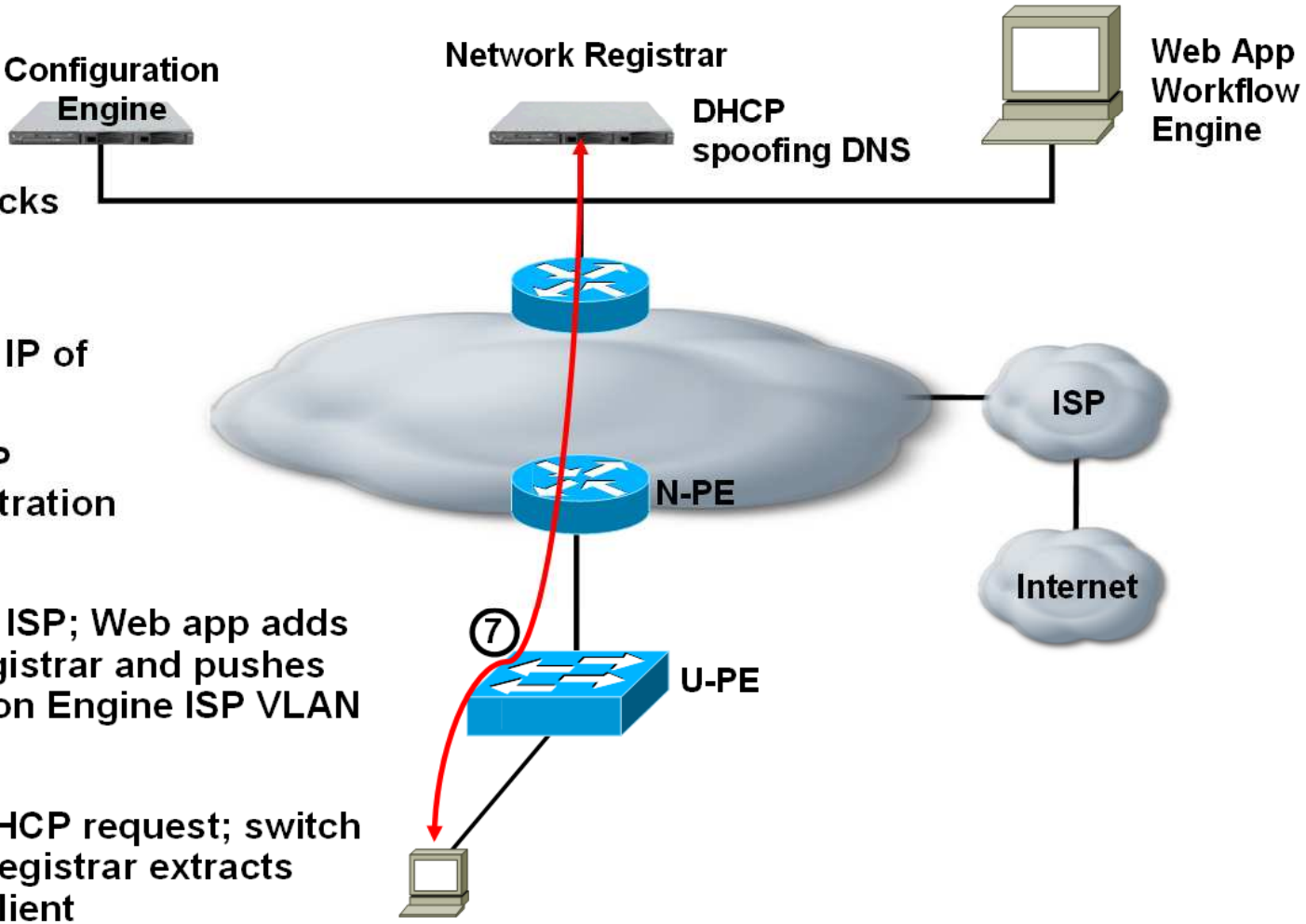
1. User plugs in PC
2. PC sends DHCP request; switch adds option 82
3. Cisco Network Registrar extracts option 82 and checks if client exists
4. No such client, so returns temporary IP address with IP of spoofing DNS server
5. User opens browser; HTTP request redirected to registration app by spoofing server
6. User registers and selects ISP; Web app adds client entry in Network Registrar and pushes through Cisco Configuration Engine ISP VLAN configuration on switch



© 2009 Cisco Systems, Inc. All rights reserved.
Cisco Public

Self-Provisioning Workflow

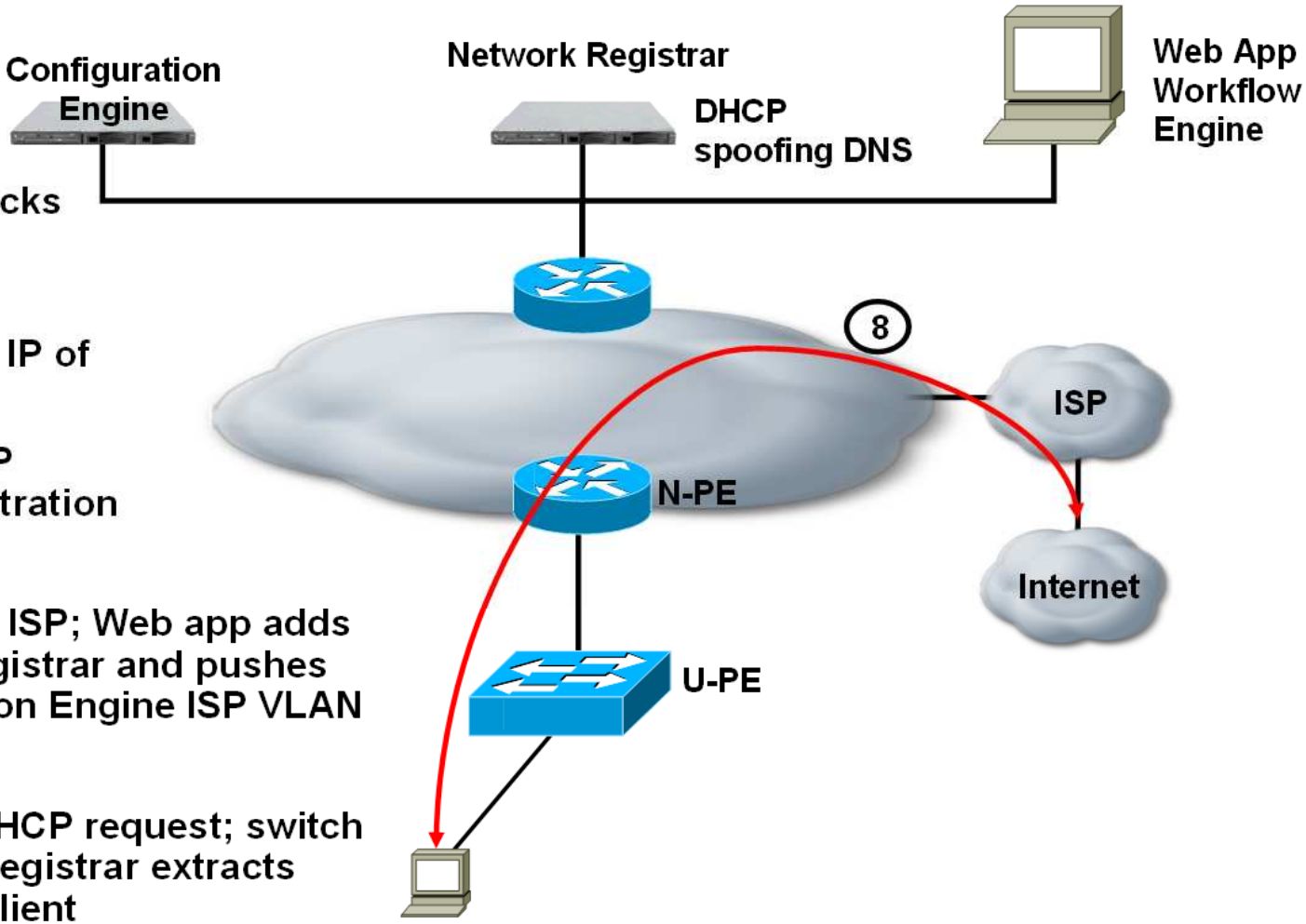
1. User plugs in PC
2. PC sends DHCP request; switch adds option 82
3. Cisco Network Registrar extracts option 82 and checks if client exists
4. No such client, so returns temporary IP address with IP of spoofing DNS server
5. User opens browser; HTTP request redirected to registration app by spoofing server
6. User registers and selects ISP; Web app adds client entry in Network Registrar and pushes through Cisco Configuration Engine ISP VLAN configuration on switch
7. User reboots; PC sends DHCP request; switch adds option 82; Network Registrar extracts option 82 and checks for client



© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Self-Provisioning Workflow

1. User plugs in PC
2. PC sends DHCP request; switch adds option 82
3. Cisco Network Registrar extracts option 82 and checks if client exists
4. No such client, so returns temporary IP address with IP of spoofing DNS server
5. User opens browser; HTTP request redirected to registration app by spoofing server
6. User registers and selects ISP; Web app adds client entry in Network Registrar and pushes through Cisco Configuration Engine ISP VLAN configuration on switch
7. User reboots; PC sends DHCP request; switch adds option 82; Network Registrar extracts option 82 and checks for client
8. Client exists, so Network Registrar provides IP address from ISP scope; user can now surf Web



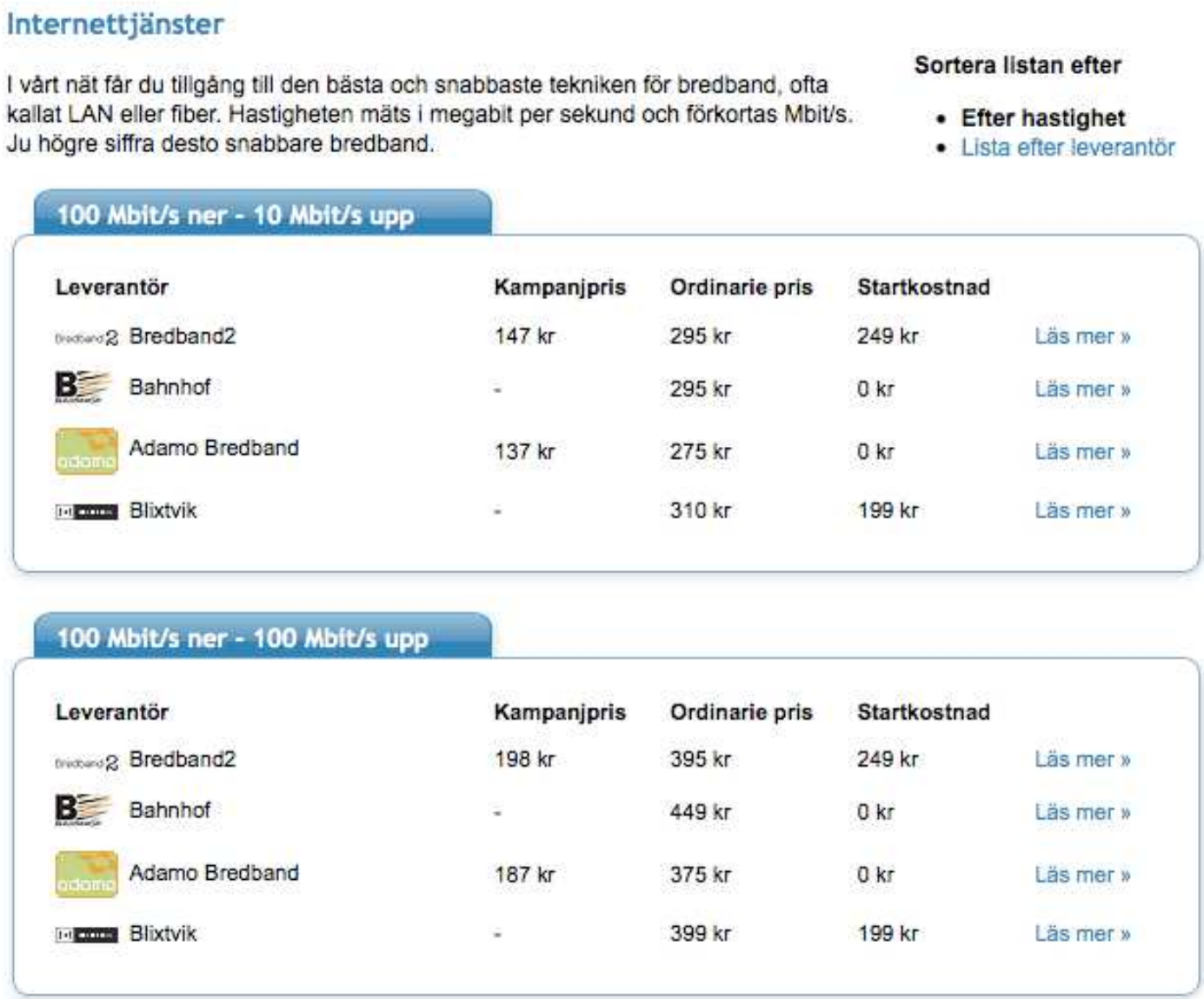
© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Subscriber Portal Example

ViaEuropa
Byt nät »
LKF Lund
Privat | Företag
Administrera dina tjänster
Aktivera ditt konto
Glömt lösenord?
Logga in
Start
Tjänster
Nyheter
Kundservice
Om ViaEuropa
Introduktion
Välkommen till LKFs bredbandsnät
Du som bor i LKF har tillgång till ett av Sveriges mest moderna bredbandsnät. Via fibertekniken kan du få några av marknadens snabbaste och billigaste bredbandstjänster. Nätet är dessutom konkurrensneutralt, vilket innebär att du kan välja mellan flera olika leverantörer. De flesta lägenheter är redan inkopplade och resten ansluts under 2008. Se LKF utbyggnadsplan »
Beställning
För att beställa en internettjänst så måste datorn vara ansluten till uttaget i din lägenhet. Detta gör att rätt internettjänst kopplas till just ditt uttag, på bara några minuter! Du kan senare gå tillbaka och ändra eller uppgradera dina tjänster.
Välkommen!
Senaste nyheterna
Ny hemsida lanserad!
2008-09-11
Nu har vi lanserat vår nya... Läs mer »
Introduktion
I vår introduktion kan du läsa mer om hur vi levererar framtidens bredband till dig. Läs mer »
INTERNET
Äkta bredband
Surfa i Sveriges högsta hastigheter genom bredbandsuttaget
TELEFONI
Ring billigare
Koppla dina telefoner till bredbandsuttaget och sänk dina kostnader
MEDIA
Underhållning
Med en snabb internet-anslutning öppnar sig en värld av nöje, när du vill!
SÄKERHET
Känn dig trygg
Tjänster för backup av dina viktiga filer till nätet, kameratjänster m.m.
Bredbandsnät med valfrihet - ViaEuropa © 2008

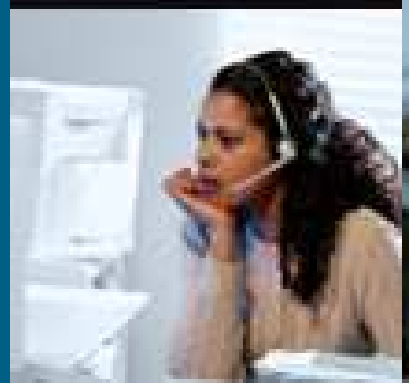
© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Subscriber Portal Example
Service Subscription


Internettjänster
I vårt nät får du tillgång till den bästa och snabbaste tekniken för bredband, ofta kallat LAN eller fiber. Hastigheten mäts i megabit per sekund och förkortas Mbit/s. Ju högre siffra desto snabbare bredband.
Sortera listan efter
Efter hastighet
Lista efter leverantör
100 Mbit/s ner - 10 Mbit/s upp
Leverantör Kampanjpris Ordinarie pris Startkostnad
Bredband2 147 kr 295 kr 249 kr Läs mer »
Bahnhof - 295 kr 0 kr Läs mer »
Adamo Bredband 137 kr 275 kr 0 kr Läs mer »
Blixtvik - 310 kr 199 kr Läs mer »
100 Mbit/s ner - 100 Mbit/s upp
Leverantör Kampanjpris Ordinarie pris Startkostnad
Bredband2 198 kr 395 kr 249 kr Läs mer »
Bahnhof - 449 kr 0 kr Läs mer »
Adamo Bredband 187 kr 375 kr 0 kr Läs mer »
Blixtvik - 399 kr 199 kr Läs mer »

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Design Considerations
Subscriber Identification



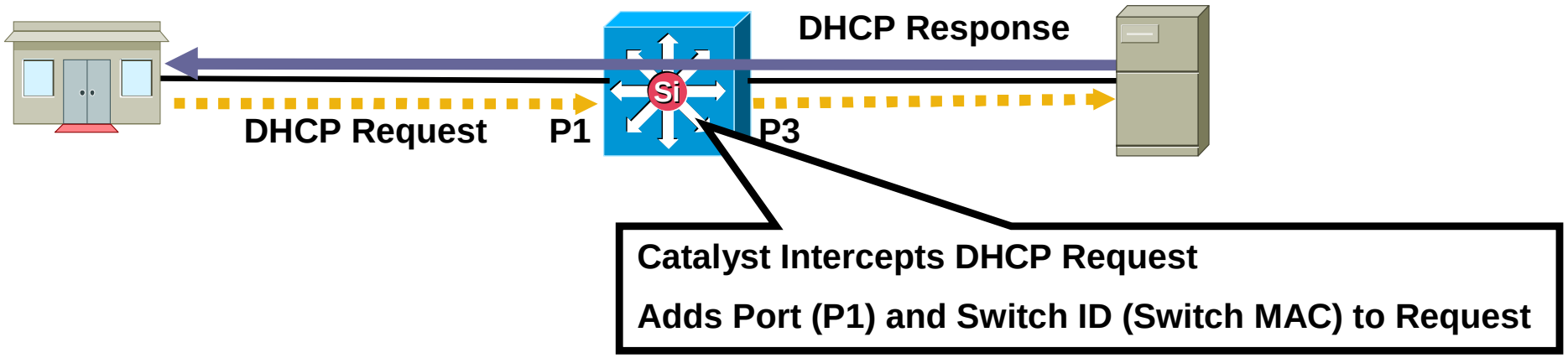
© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Subscriber Identification

- Subscriber & Network elements need to be identified for
  - Access control / Policy Enforcement
  - Security / Trace-ability
  - Billing
- This can be done via MAC addresses
- Or via User login using SSG (Service Selection Gateway) or a Portal
  - Requires Service Portal for Authentication, not transparent
- Via PPPoE and Radius
  - Requires BRAS, and PPPoE Client
- Or via support of DHCP Option 82
  - Access switch automatically populates Option 82 with switch and port ID when relaying DHCP request

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

DHCP Interface Tracker (Option 82)



- Subset of DHCP Snooping feature
- Used by Service Providers to:

  Identify each user

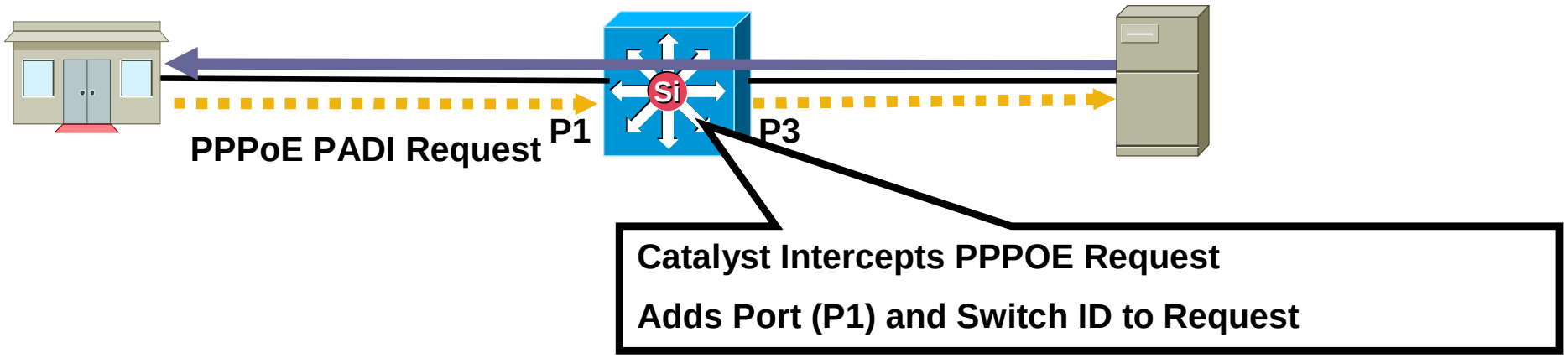
  Perform subscriber management

  Assign IP addresses based on switch port and subscriber info
- How does it work:

  Port (Module/Port/VLAN) and local switch info are added to the incoming DHCP the request

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

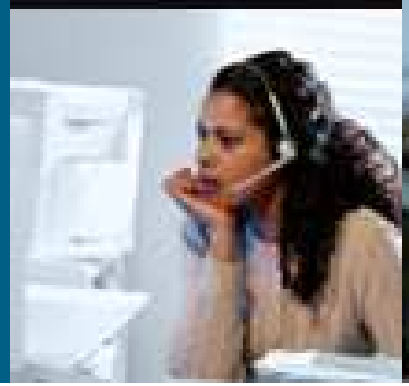
PPPoE Intermediate Agent



- Used by Service Providers to:
  - Identify each user based on location
    - CPE do not need to be pre-configured with User Data
  - Perform subscriber management
  - Assign IP addresses based on switch port and subscriber info

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Design Considerations
Subscriber Isolation & Security



© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Subscriber Isolation & Security

- Security is a prime consideration within any Public switched network
  - One user should not affect any other user
  - Users should not be able to affect the network integrity
- Ethernet as a technology is inherently insecure due to the “Plug and Play” nature of Ethernet
- Irrespective of Architecture, Ethernet services use Ethernet technologies
  - 802.1q, 802.1w/s, 802.1d, MAC-Address Learning, etc

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Potential Security Threats

- Security attacks generally fall into one of the following categories:

  Intrusion: The attacker attempts to gain unauthorized access to network resources, including traffic from other customers

  Common Examples:

  Rogue DHCP server

  IP & MAC address spoofing

  ARP spoofing (Man-in-the-Middle) Attack

  Denial of Service (DoS): The attacker attempts to disrupt normal network and service operations

  Common Examples:

  MAC attacks (CAM table overflow)

  Broadcast storms

  L2 PDU storm (STP, LACP, PAgP, etc..)

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Ethernet Access Security Threats

- Attack targets can be divided into three main categories:

Subscribers	Access Nodes	Infrastructure
Layer 2 service isolation across switches	L2 Control Protocol Attack (STP, CDP, VTP, etc…)	Man-in-the-Middle attacks on critical management traffic
Non intentional forwarding of traffic between UNI ports	MAC Flooding / Overflow	Unauthenticated access to the switch configuration file
DHCP Rogue Server	DHCP Resource Overflow	Unconfigured Ports providing network access
IP & MAC Address Spoofing	Unicast, multicast, or broadcast storms	Unauthorized network access, junk traffic
ARP Spoofing (Man-in-the-Middle)	Infected users flooding the network / Malicious users attacking the Priority traffic queue	Unauthenticated network access by client devices

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Subscriber Security

- One of the biggest concerns in using a shared Ethernet Access device for multiple customers is how to prevent one customer from affecting another customer

Security Threat:	
Layer 2 Isolation across switches	Subscriber Isolation
Non intentional forwarding of traffic between UNI ports	
DHCP Rogue Server	Intrusion
IP & MAC Address Spoofing	
ARP Spoofing (Man-in-the-Middle)	

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Subscriber Security Solutions

Security Threat:	Solution
Layer 2 Isolation between UNI ports	Private VLANs or UNI/NNI ports
Layer 2 Isolation between Access Node	Private VLANs Trunk
DHCP Rogue Server	DHCP Snooping
IP & MAC Address Spoofing	DHCP Snooping + IP Source Guard
ARP Spoofing	DHCP Snooping + Dynamic ARP inspection

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Private VLAN

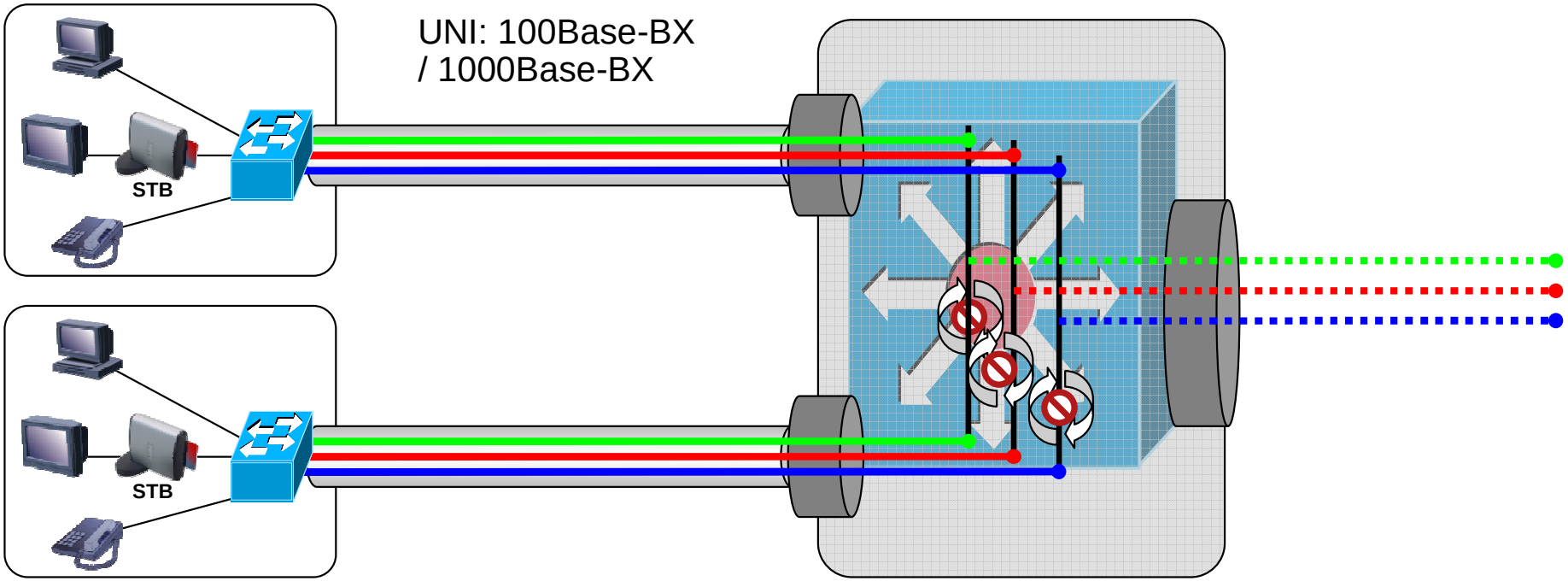
- **What It Does:**

  Prohibit switching traffic between subscriber UNI (UNI traffic only forwarded to promiscuous or NNI port)

  Configurable per Service-VLAN (can be multiplexed over a physical port).

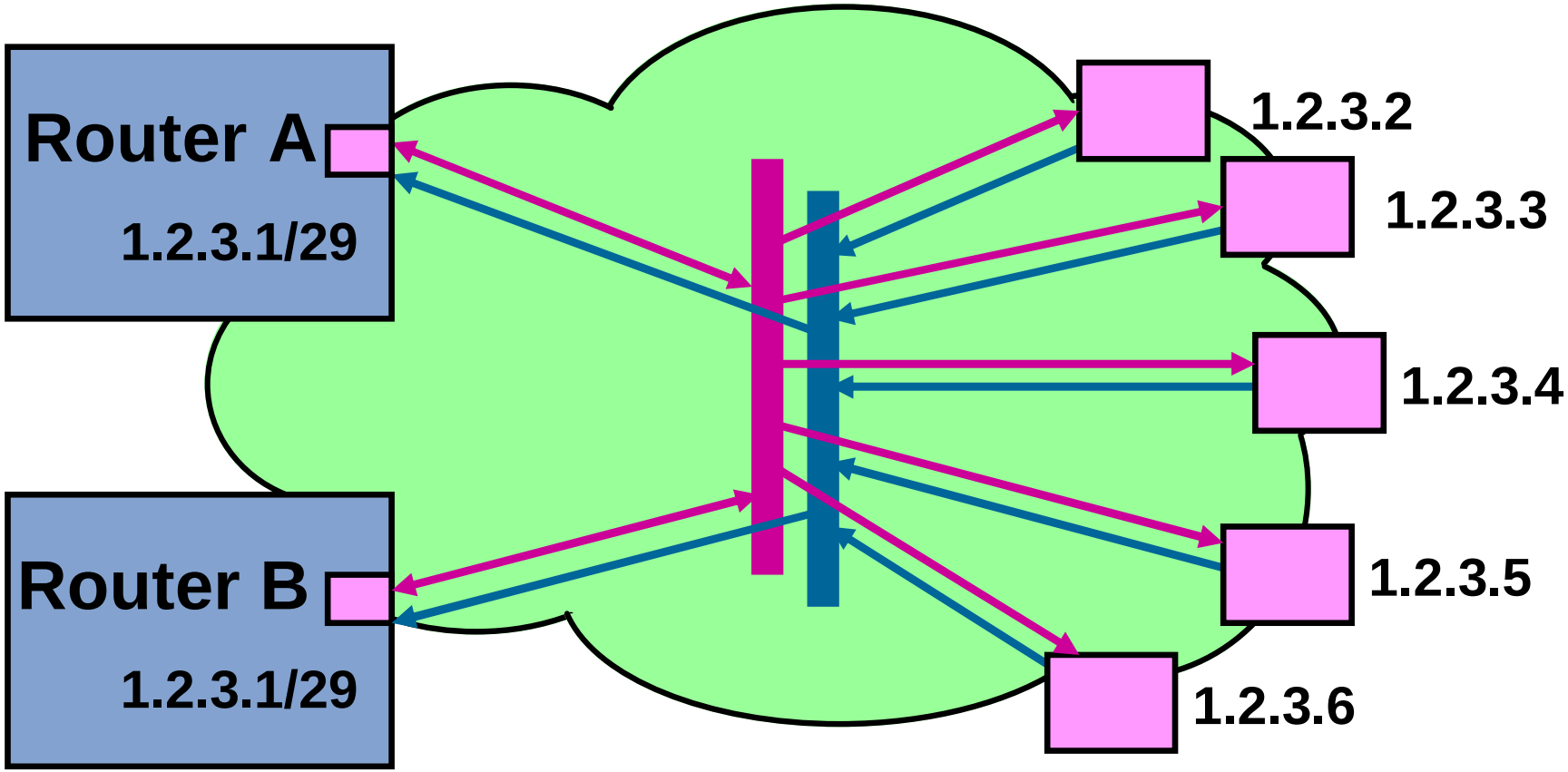
- **Benefit:**

  Provide simple Isolation between UNIs in a N:1 VLAN model



© 2009 Cisco Systems, Inc. All rights reserved.

Private VLAN



- A few Routers, many Subscribers.
- Two P-VLANs, one “Down”, and one “Up”.
- Can be shared between and across switches (e.g. in a ring)
- Supported on Catalysts ME3400, 3750, 4500 and 6500/7600

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

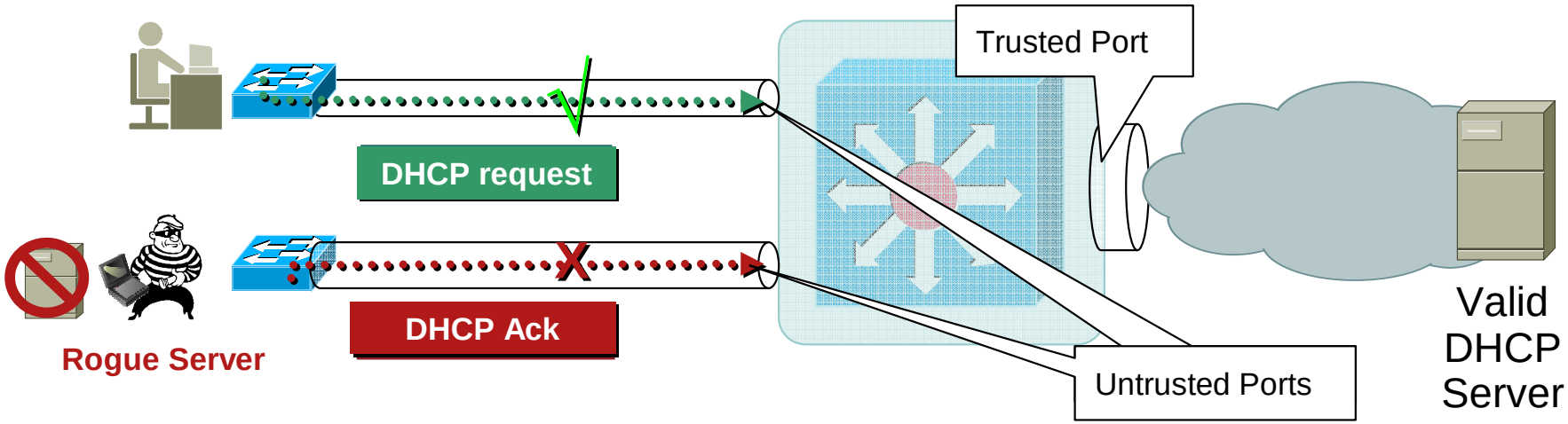
DHCP Security

- DHCP is used to provision network elements (HAG, STB,…) and subscriber devices
- Private VLAN isolates subscribers from one other, but does not protect first L3 hop
- DHCP Snooping on first access switch will accomplish this!
- Access Switch will snoop (bridge) the DHCP request and replies in order to build a MAC-to-IP binding table
- Results in environment which is as secure as L3
- State is setup automatically and maintained inside the network

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

DHCP Snooping

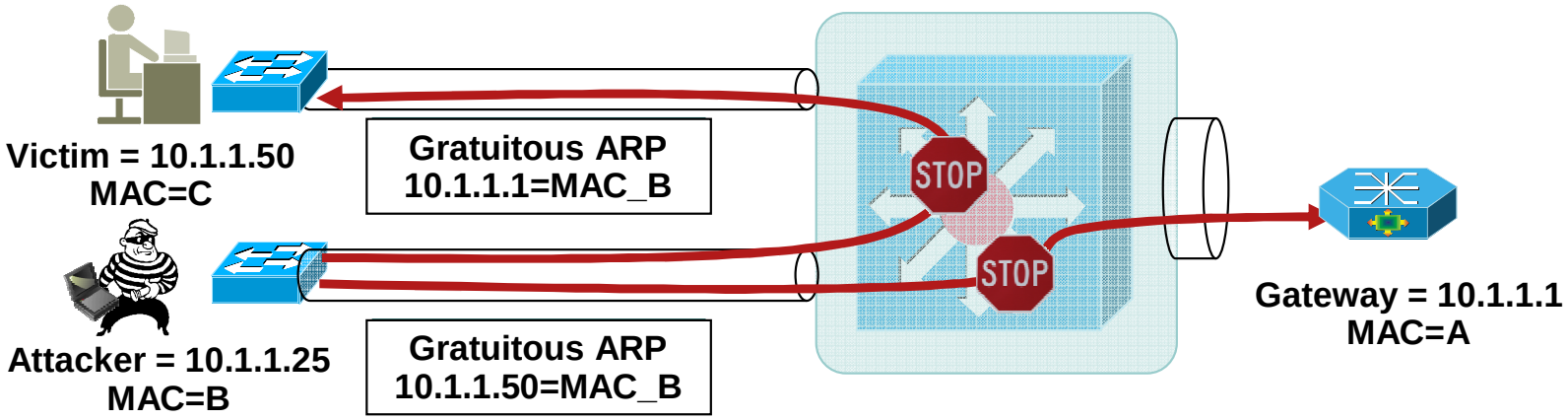
- **Risk :**
  - A rogue user spoof a DHCP server and send fake DNS, IP, Default. Gateway



- Prevent denial of service (DoS) attacks based on DHCP protocol
  - Malicious—user pretends to be the Network DHCP Server
  - Misconfiguration—user configures router (DHCP server) incorrectly
- How it works:
  - The access switch only forwards DHCP requests from access ports (untrusted ports); All other types of DHCP traffic from access ports is dropped
  - If the server is not local to the Catalyst Switch, trust the uplink port
  - DoS attack can be prevented by rate limiting the DHCP packets on access ports

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

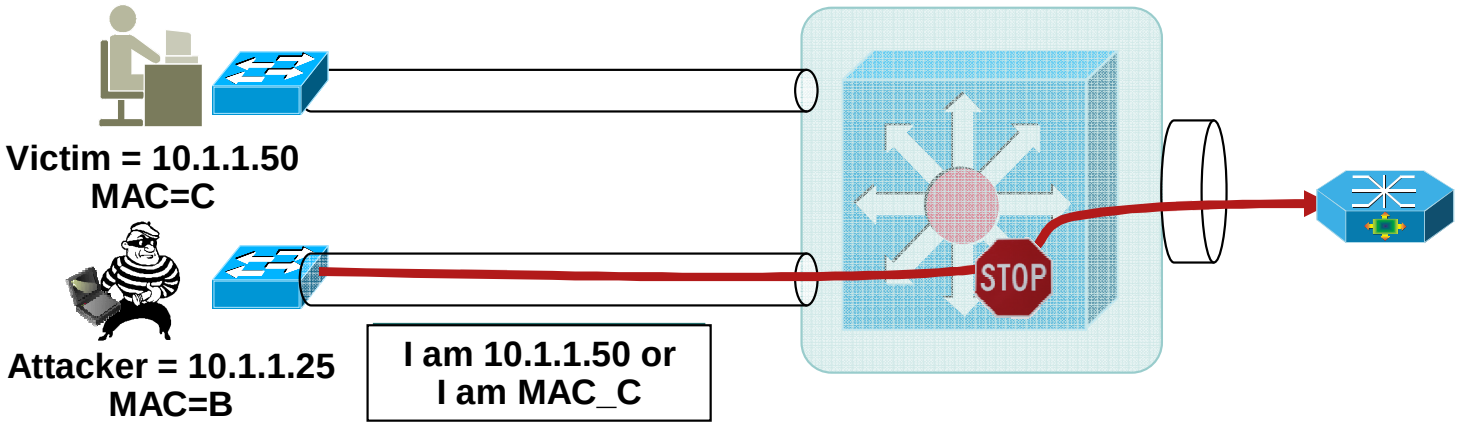
ARP attacks (ARP spoofing)



- **Risk:**
  - MITM attack, malicious user sends Gratuitous ARP and poisons ARP table
- **Solution:**
  - Dynamic ARP Inspection – tracks MAC-to-IP using DHCP binding table, and drop bogus ARPs request.

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Spoofing attacks (IP, MAC spoofing)



- **Risk:**
  - Malicious subscriber usurps MAC or IP address
- **Solution:**
  - IP Source Guard – tracks {MAC, IP, VLAN, port} association using DHCP binding table, and drop bogus IP packets or L2 frames with dynamically installed ACLs

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Access Nodes Security

- Security Threats often target the infrastructure itself in order to slow down or halt operation of the device under attack
- Denial-of-Service attacks and flooding attacks are most common

Security Concern:
L2 Control Protocol Attack (STP, LACP, PAgP, CDP, VTP, etc…)
MAC Flooding / Overflow
DHCP Resource Starvation
Unicast, multicast, or broadcast storms
Infected users flooding the network / Malicious users attacking the Priority traffic queue

Denial of Service

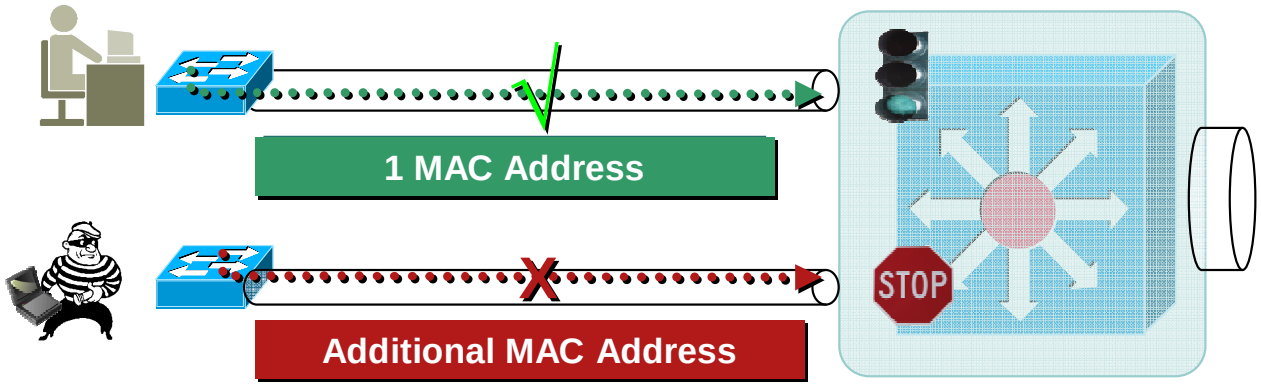
© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Access Node security Solutions

Security Concern:	Solution
L2 Control Protocol Attack (STP, LACP, PAgP, CDP, VTP, etc…)	Control Plane Policing
MAC Flooding / Overflow	Port Security & Configurable Per VLAN MAC Learning
DHCP Resource Starvation	Port Security + DHCP Snooping
Unicast, multicast, or broadcast storms	Storm Control
Infected users flooding the network / Malicious users attacking the Priority traffic queue	Rate-limiting, Priority policing

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Mac attacks (mac table overflow)



- **Risk:**
  - Defeat SP Nodes resources by overflowing MAC table (CAM)
- **Solution:**
  - Port Security – Limits the amount on MACs on an interface. Flooding attack will lock down port and send SNMP trap

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

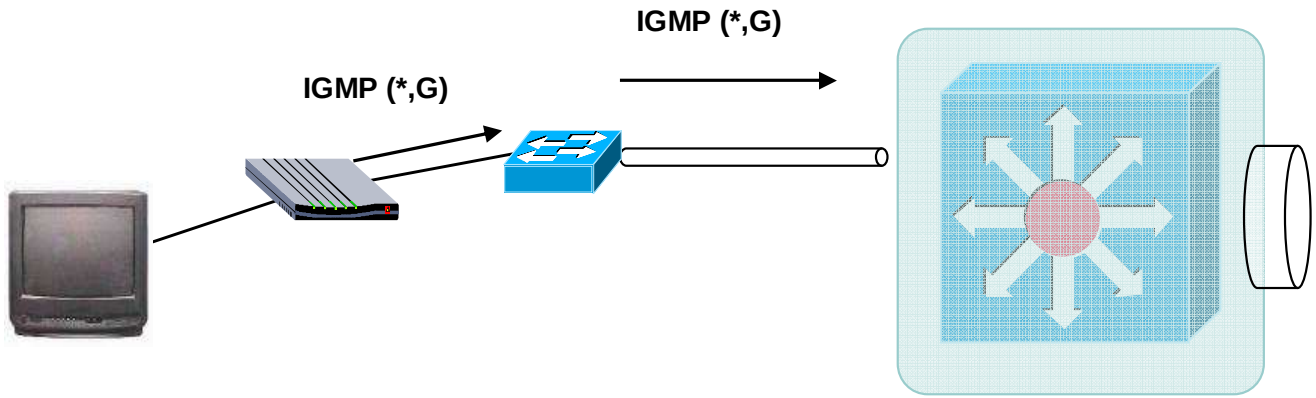
Port Security

- Available on ME3400, Catalyst 4500 and Catalyst 6500
- Allows to limit the number of MAC addresses on an access port
- MAC addresses can be statically configured or learnt dynamically
- Aging timer is now available
- Security violation action configurable
- Ports do not forward packets with source addresses outside the group of defined addresses => Prevents MAC Spoofing!

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Controlling multicast traffic

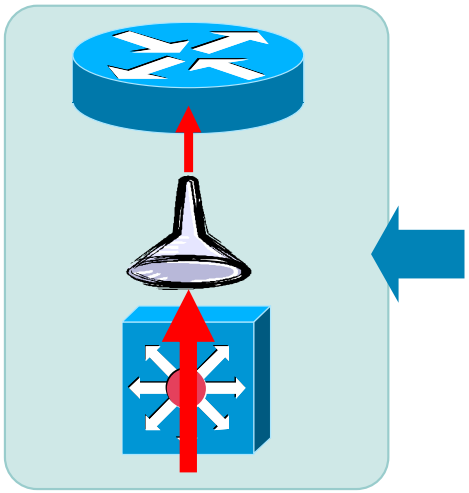
- **Options:**
  - Service related
    - ✓ Restrict access to a list of multicast groups (IGMP filter list)
    - ✓ SSM mapping to force the source address
  - Control plane:
    - ✓ Filter PIM packets on the UNI (IGMP leave/reports only)
    - ✓ Rate-limit IGMP packets punted to CPU



© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

CPU and Control Plane protection

- **Options:**
  - Provide an additional layer of CPU protection and Control
  - CPU rate limiters to control traffic types
  - Control Plane Policing (CoPP) to filter and rate-limit control plane traffic

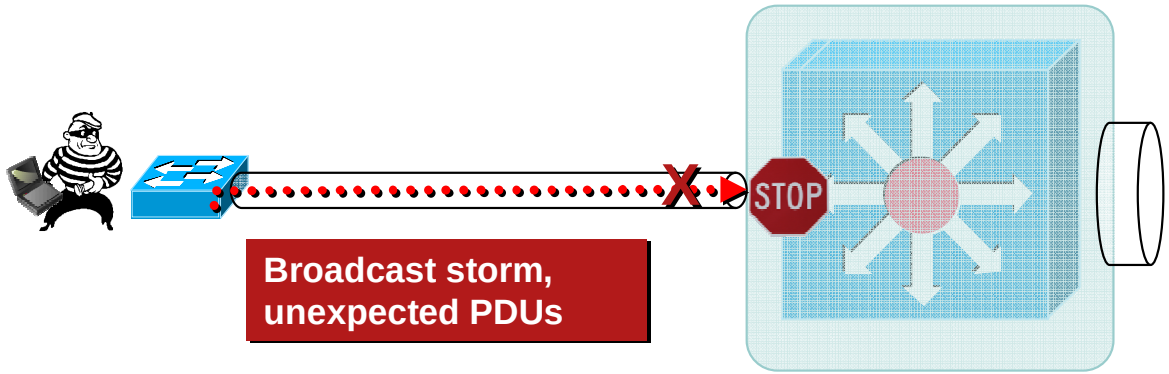


Apply Inbound QoS Policy via CoPP
CPU rate limiters for targeted unicast and multicast traffic destined to control plane

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Countering L2 protocol attackes

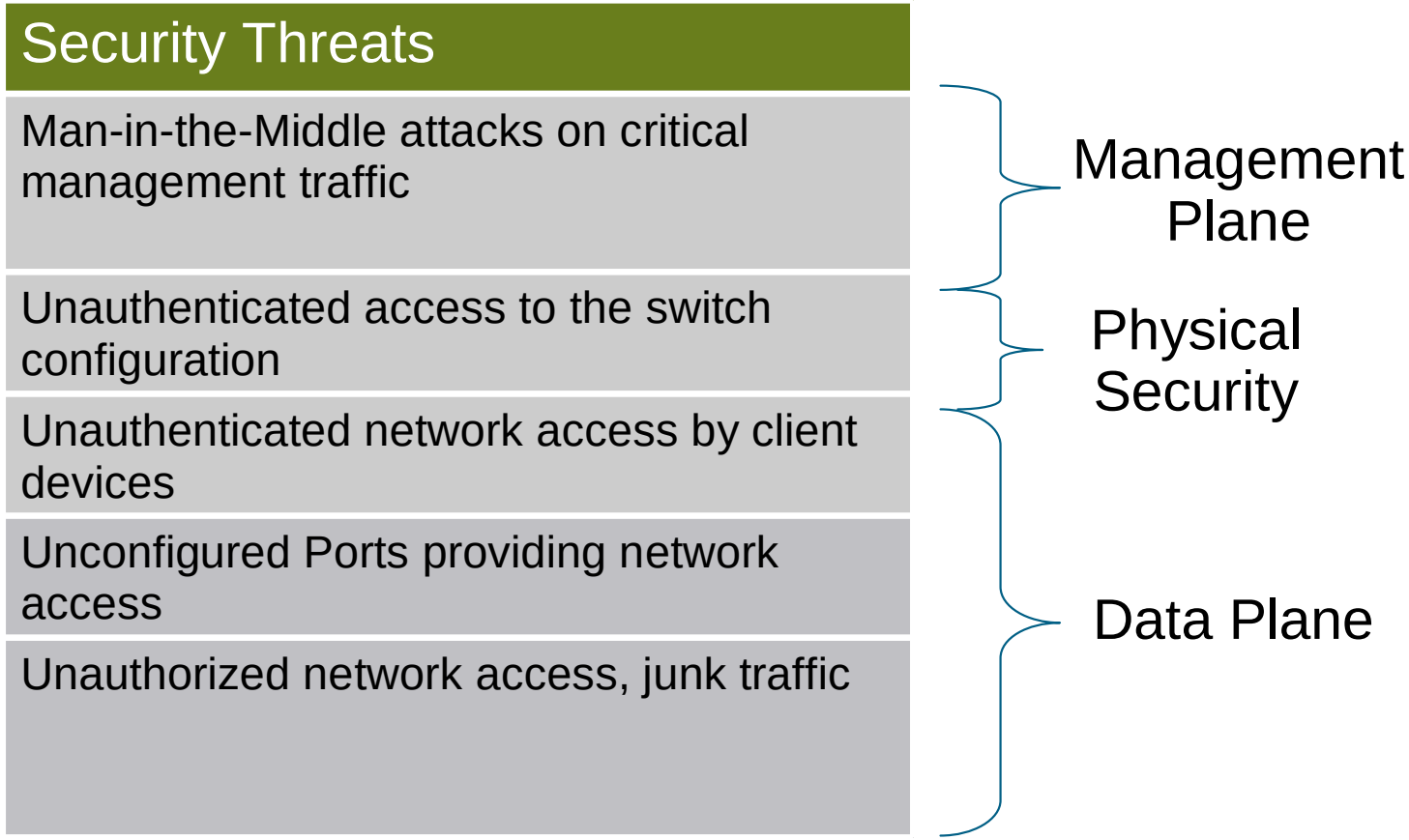
- **Options:**
  - Service related:
    - ✓ limits the volume of broadcast, multicast traffic and/or unicast traffic from the customer, trigger action when thresholds are exceeded
  - Control plane:
    - ✓ Filter BPDUs in/out (BPDU-filtering)
    - ✓ RootGuard to prevent a port from becoming root port or blocked port
    - ✓ Loopguard, etherchannel guard ...



© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Infrastructure Security

- Infrastructure attacks exploit insecure data, control and management planes as well as weak physical security
- It is essential to ensure that only valid traffic is allowed through the switch through filtering and blocking. This must be done at the edge of the SP network e.g. Metro Access switches


Security Threats
Man-in-the-Middle attacks on critical management traffic
Unauthenticated access to the switch configuration
Unauthenticated network access by client devices
Unconfigured Ports providing network access
Unauthorized network access, junk traffic
Management Plane
Physical Security
Data Plane

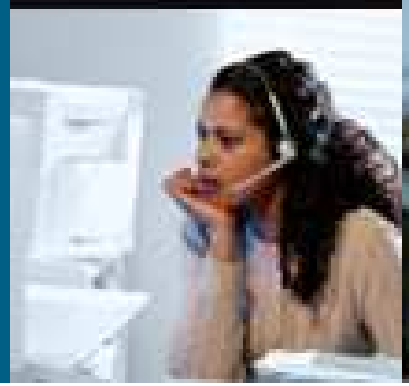
© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Infrastructure Security Solutions

Security Threats	Solution
Man-in-the-Middle attacks on critical management traffic	Out-of-Band Management, SNMPv3, SSH, per-command AAA
Unauthenticated access to the switch configuration	Password recovery disable
Unauthorized network access, junk traffic	Access Lists

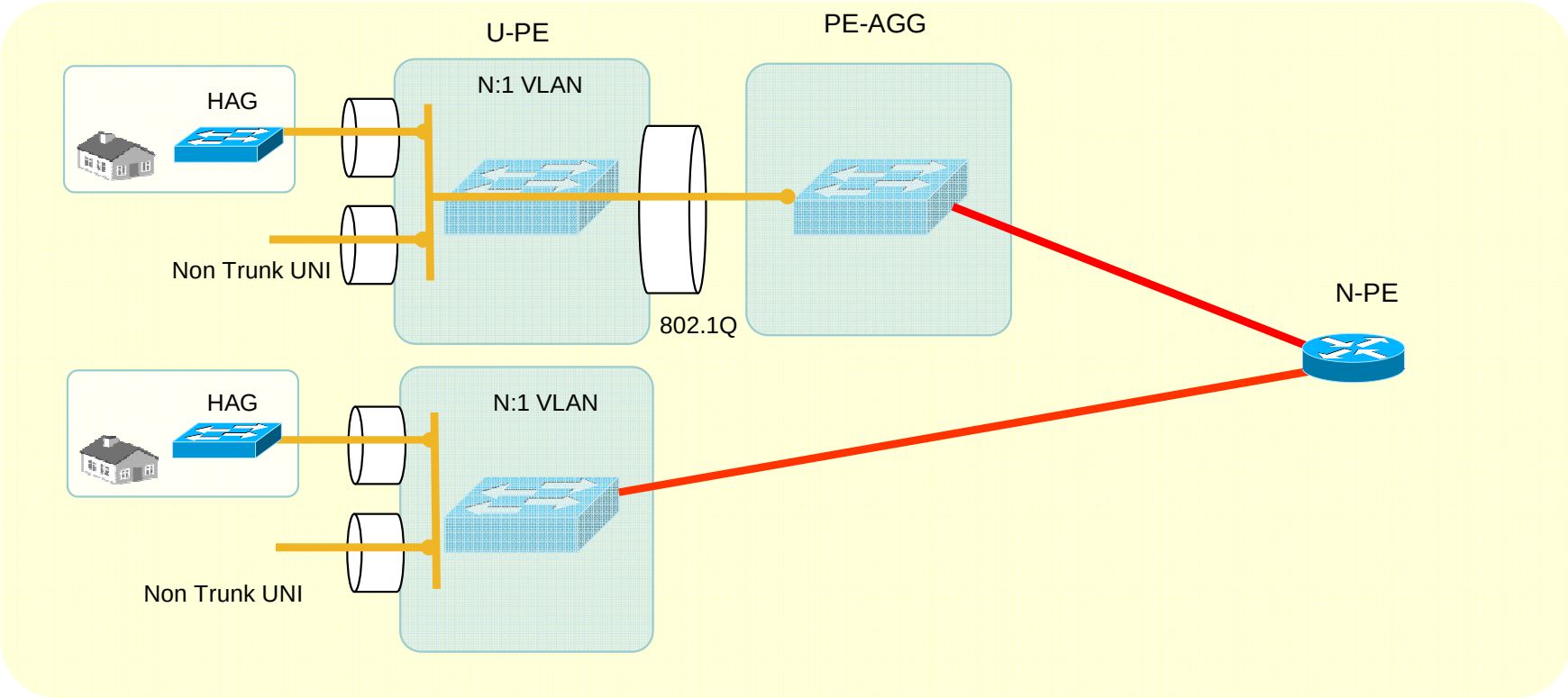
© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Design Considerations
Network Resilience



© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Network Resilience



- **802.1D Spanning Tree for Layer 2 portions of the network**

  Rapid Spanning Tree and Multiple Spanning Tree enhance recovery

- **IP Routing Protocols for Layer 3 portion of the network**

  Cisco U-PE support full range of protocols (ISIS, OSPF, EIGRP,..)

- **Resilient Ethernet Protocol (REP) for access rings**

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Spanning Tree… The Spawn of the Devil? (Not Anymore!)

- Convergence and Scalability are extremely improved through 802.1w and 802.1s (now part of 802.1D-2003 and 802.1Q-2003)
  - Rapid Convergence (sub-second) and support for multiple STPs
  - Switches are ‘built’ for Spanning Tree
  - Special input and output queues on ports for STP
  - Special CPU queues and CPU handling for STP
  - All links are full-duplex and collision free—a BPDU send will always get received
- Do not span a VLAN across too many switches
  - Not even the management VLAN
  - No need to use a single management VLAN for the entire topology

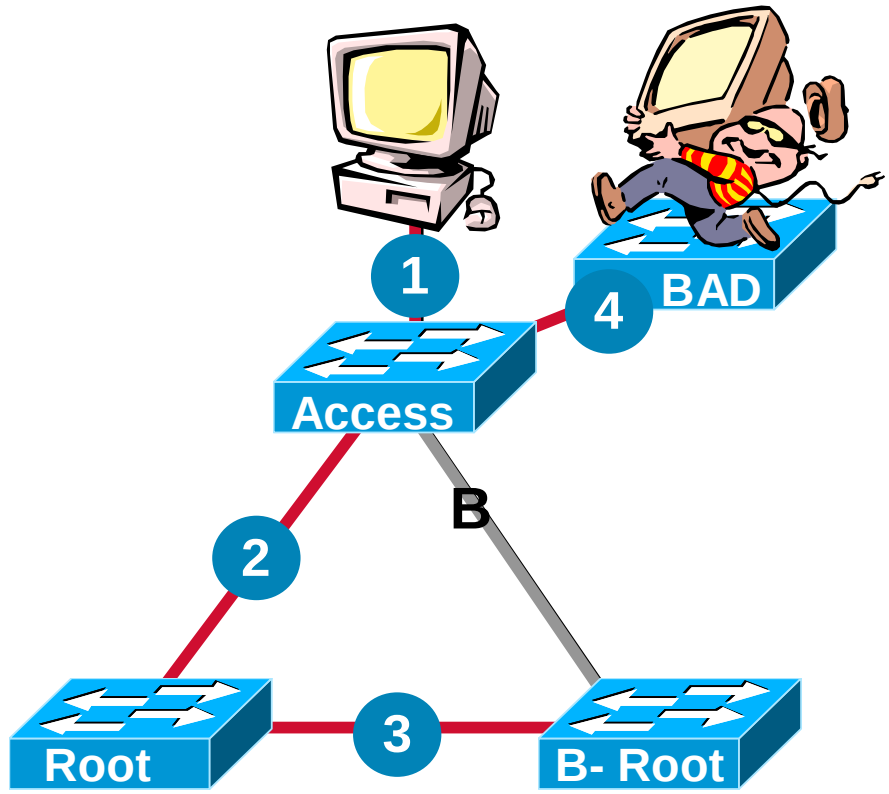
© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Cisco Spanning Tree Toolkit

1. **PortFast**
   for Edge Ports
   (0-30 secs)

2. **UplinkFast**
   for direct Root link failure
   (3-30 sec)

3. **BackboneFast**
   for indirect link failure
   (30 to 50 sec)



Now standardized with 802.1w/.1d

RootGuard:
prevents an external switch from becoming root

4. **BPDU-Guard:**
   Disables a portfast non-trunk port if it receives a BPDU

BPDU Filtering:
Filters outgoing and received BPDUs

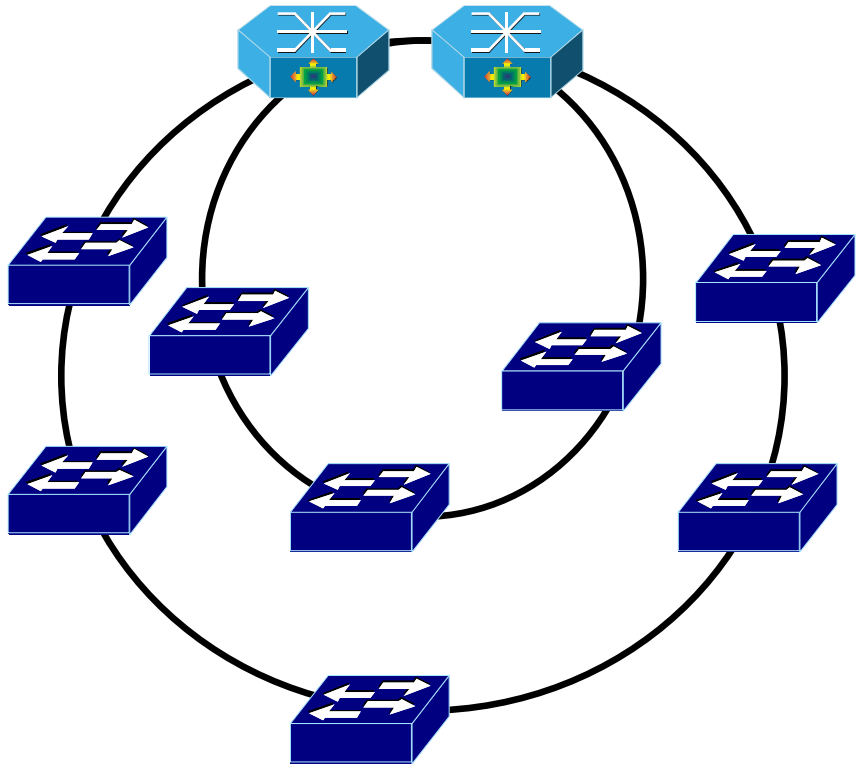
© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Resilient Ethernet Protocol

Provide a solution for robust and predictable layer 2 convergence for Metro Ethernet ring networks

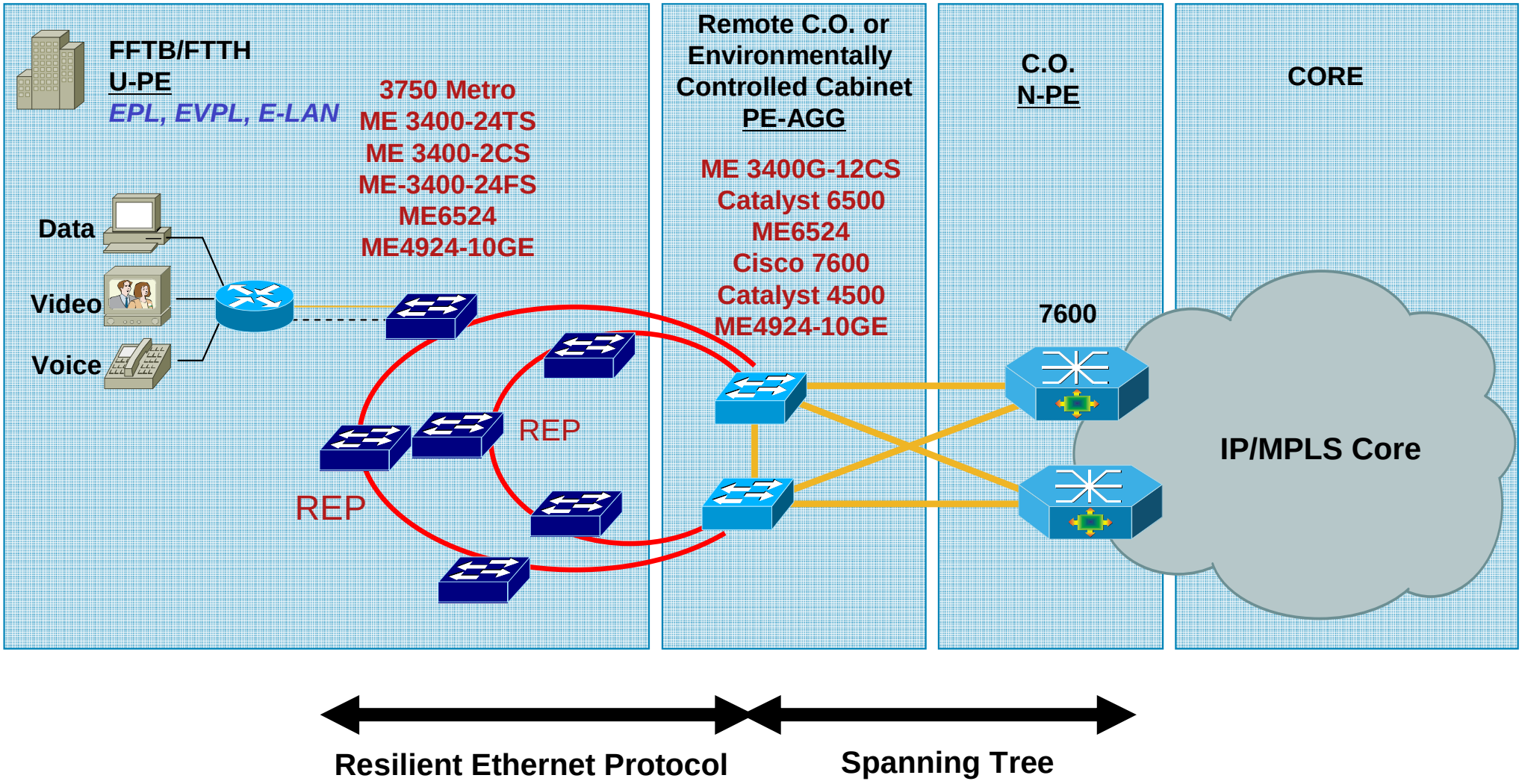
REP is designed to address:

- Fast re-convergence for simple ring networks **(<200ms)**
- No Spanning Tree (STP)
- VLAN load balancing
- Manual configuration for predicable failover behavior
- Supported on existing hardware platforms



© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

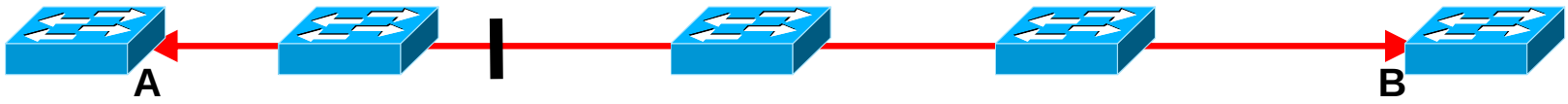
Cisco REP Solution Deployment Example



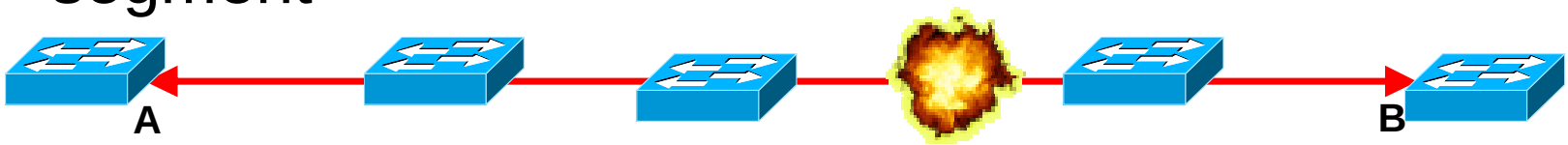
Fast Convergence from the access to the N-PE

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

REP is a Segment Protocol



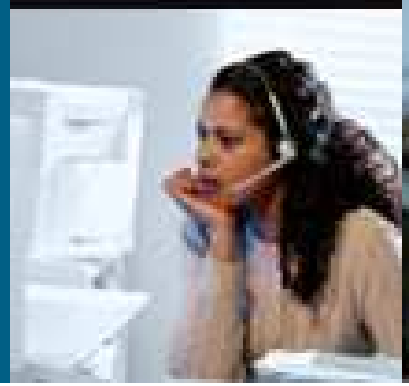
- Ports are explicitly configured to be part of a segment.
- When all the links in the segment are operational, a blocked port is determined so that there is no connectivity between the edges A,B through the segment



- If a failure occurs within the segment, the blocked port goes forwarding

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Design Considerations
Quality of Service (QOS)



© 2009 Cisco Systems, Inc. All rights reserved.

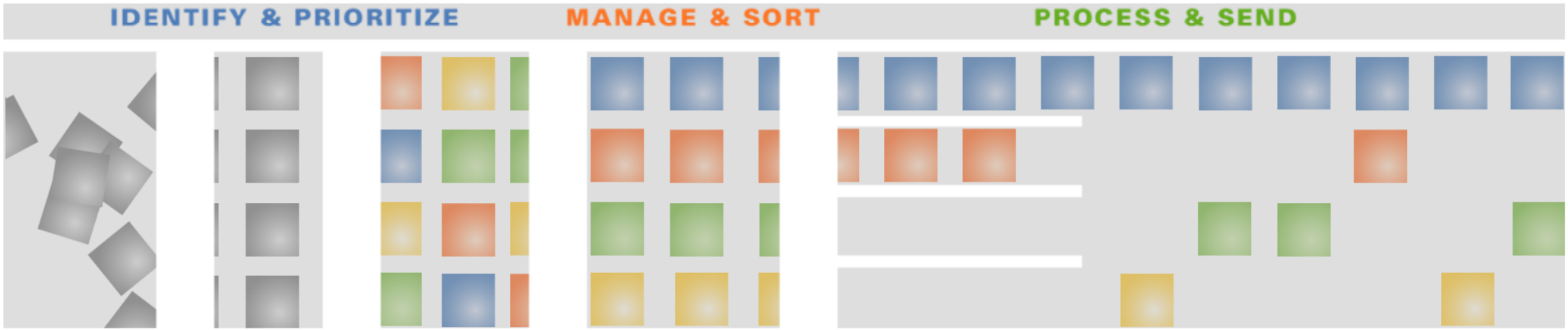
FTTH QoS Strategy

- End-to-End QoS based on DiffServ model
- Traffic Marking
  - Rely on classification capability of access switch
  - Smart IP addressing makes this extremely easy
  - Or…rely on CPE device (not recommended)
- Per service policing can be done on access switch
  - Certainly needed for Voice and Video
- Per class queuing on customer facing ports
  - Voice added to Strict Priority Queue (Policing is needed!)
  - Video added to Weighted Round Robin Queue with highest weight
- Per class queuing and congestion avoidance on uplinks (strict priority queuing, WRR queuing, weighted RED or taildrop)
- Fairness between subscribers can be achieved using per-subscriber In/Out contract policing and WRED at the Internet access router

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

How Packet DiffServ QoS Works

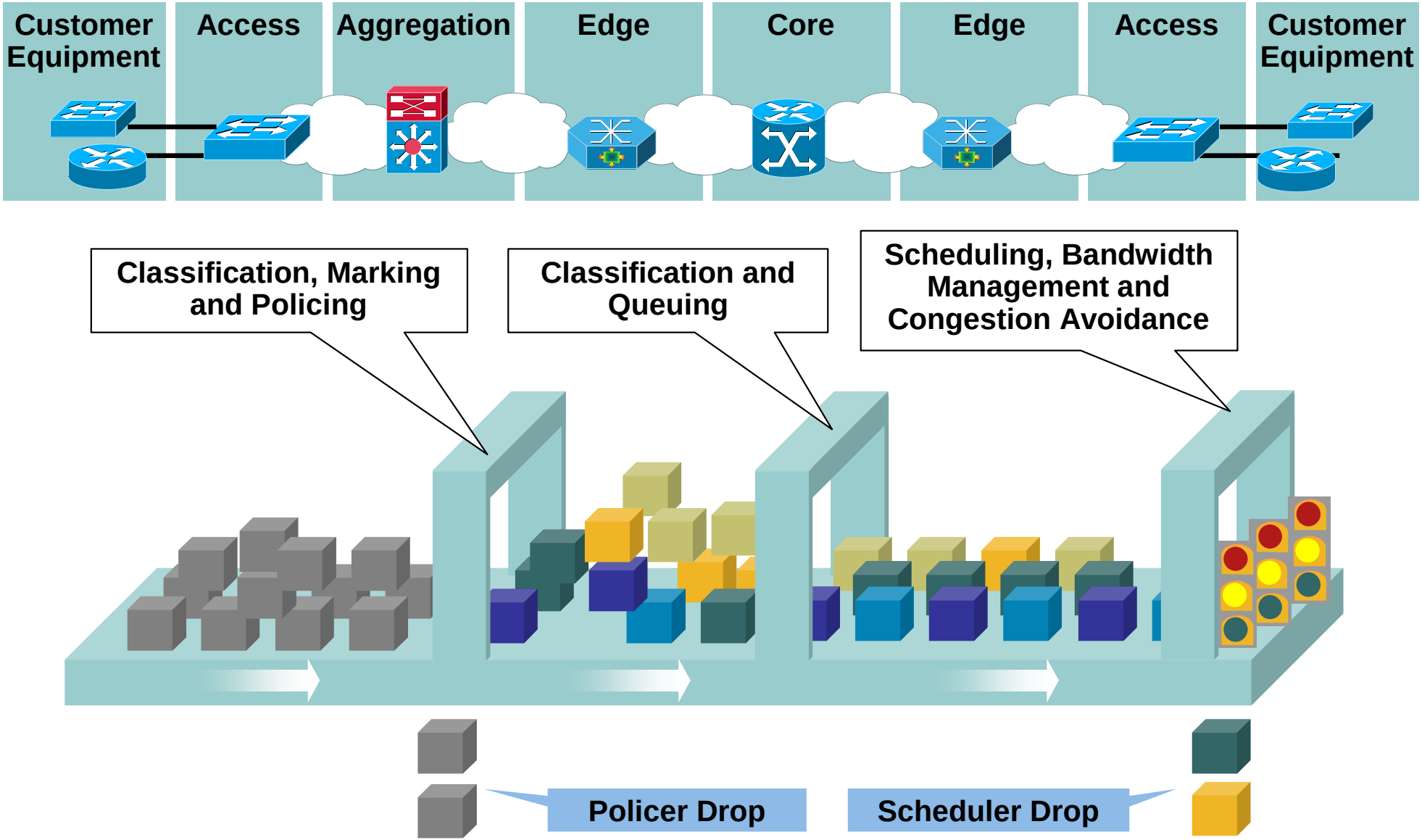
An Intelligent Delivery System



- Enforce Trust Boundary or Classify
- Manage Rates and reclassify if required
- Schedule and Transmit based on requirements

© 2009 Cisco Systems, Inc. All rights reserved.
Cisco Public

QoS Mechanisms—Example



© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Q and A

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Meet The Expert

To make the most of your time at Cisco Networkers 2009, schedule a Face-to-Face Meeting with a top Cisco Expert.

Designed to provide a "big picture" perspective as well as "in-depth" technology discussions, these face-to-face meetings will provide fascinating dialogue and a wealth of valuable insights and ideas.

Visit the Meeting Centre reception desk located in the Meeting Centre in World of Solutions

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Recommended Reading

- There are currently no Cisco Press Books recommended for this Presentation - please browse the Cisco Company Store for suitable titles

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public

Thank You

CISCO